FFI-RAPPORT

16/02319

Metode for klassifisering av havneanlegg og en overordnet trusselvurdering

–

Maren Maal
Kjersti Brattekås
Siw Tynes Johnsen[1]
Janita Bruvoll
Leif D. Riis[2]

[1, 2] Forsvarsbygg

Metode for klassifisering av havneanlegg og en overordnet trusselvurdering

Maren Maal
Kjersti Brattekås
Siw Tynes Johnsen[1]
Janita Bruvoll
Leif D. Riis[2]

[1, 2] Forsvarsbygg

Forsvarets forskningsinstitutt (FFI) 2. desember 2016

Emneord

Havnesikring
Verdivurdering
Risikobasert tilsyn
Klassifisering
Trussel

FFI-rapport
FFI-RAPPORT 16/02319

Prosjektnummer
5161

ISBN
P: ISBN 978-82-464-2854-3
E: ISBN 978-82-464-2855-0

Godkjent av
Kjersti Brattekås, *forskningsleder*
Janet M. Blatny, a*vdelingssjef*

Sammendrag

På oppdrag fra Kystverket (KYV) har Forsvarets forskningsinstitutt (FFI) og Forsvarsbygg futura ved Nasjonalt kompetansesenter for sikring av bygg (NKSB) utarbeidet en metode for klassifisering av norske havneanlegg. I tillegg inkluderer rapporten anbefalinger til KYV sitt risikobaserte tilsyn.

Formålet med denne studien er todelt. I henhold til oppdragets mandat skal studien være veiledende i forhold til "(i) det risikobaserte tilsyn KYV fører i norske havner og havneanlegg av deres sikringsregimer, og (ii) ved fastsettelse av det maritime sikringsnivået i norske havner og havneanlegg, spesielt ved et økt generelt trusselnivå". FFI og NKSB har utarbeidet en metode for klassifisering av havner og havneanlegg basert på kritikalitet, det vil si hvor kritisk havnen eller havneanlegget er.

Gjennom arbeidsmøter og innspill fra KYV har det blitt utviklet ulike kriterier for å bedømme kritikalitet med tilhørende rangeringstabeller. Noen eksempler på slike kriterier er antall årlige passasjerer, hvilken type gods som blir lagret og fraktet og havneanleggets strategiske betydning. Åtte rangeringstabeller blir brukt for hvert enkelt havneanlegg for å bestemme hvilken samlet poengsum de får og dermed hvilken sikringsprofil de tilhører (gruppe 1 er minst risikoutsatt, gruppe 2 er mer utsatt og gruppe 3 er svært utsatt). Deretter må havneanleggets poengsum vurderes opp mot de andre International Ship & Port facility Security code (ISPS)-havneanleggene i havnen. Alle havneanlegg i en gitt havn må dimensjoneres etter den høyeste poengsummen.

FFI og NKSB har i denne rapporten gjennomført en litteraturstudie og en overordnet trusselvurdering der vi beskriver generelle trusseltrender innen maritim sektor. Trusselvurderingen fokuserer på kategoriene terror, etterretning, sabotasje og annen kriminalitet. FFI og NKSB har benyttet seg av trendrapporter fra Kripos, Politiets sikkerhetstjeneste, Etterretningstjenesten, forskningsrapporter fra FFI samt internasjonale databaser over terrorhendelser. FFI og NKSB har også hatt en samtale med PST om generelle trusseltrender i Norge. KYVs hovedkontor har bidratt med sitt hendelsesregister med ulike typer trusler og sikringshendelser i deres sektor.

Denne studien anbefaler at Kystverket baserer sine risikobaserte tilsyn på resultatene fra klassifiseringsmetoden, samt havneanleggenes egne gjennomførte sårbarhetsvurderinger. Hyppigheten av tilsyn bør vurderes med hensyn til både hvor kritisk havnen er og erfaringer fra tidligere tilsyn. Grunnlaget for tilsynet bør være bredt forankret, og det anbefales derfor at de ulike havneanleggene selv er involvert i prosessen med klassifiseringen og sårbarhetsvurderingene. Rapporten presenterer også en modell for risikobasert tilsyn. Modellen og anbefalingene baserer seg på bidrag fra relevant faglitteratur og på erfaringsbasert kunnskap.

Summary

The Norwegian Defence Research Establishment (FFI) and the National Centre for Protection of Buildings (NKSB) have developed a method for classifying Norwegian ports and port facilities, and given recommendations on how best to conduct risk-based supervision. The research has been funded by the Norwegian Coastal Administration (KYV).

The purpose of this study is twofold. According to the mission's mandate the study should provide guidance in relation to “(i) the risk-based supervision conducted by KYV in Norwegian ports and port facilities of their security regimes, and (ii) determining the maritime security level in Norwegian ports and port facilities, particularly if the general threat level has increased". FFI and NKSB have developed a method for classifying port facilities based on criticality, i.e. how critical the port or port facility is.

Through workshops and input from KYV the working group has developed various criteria for criticality, which includes ranking tables. Examples of criteria developed include the number of annual passengers, the type of goods being stored and transported, and the port facility's strategic importance. Eight ranking tables are used for each port facility to determine the overall score, and thus determine which security profile the port facility belongs to (group 1 is least at risk, group 2 is more vulnerable, and group 3 is high risk). The score for the port facility must be weighed against the scores of the other International Ship & Port facility Security code (ISPS) port facilities in the harbor. The highest score in a port will affect the scores of all the other port facilities.

FFI and NKSB have in this report conducted a literature study and a general threat assessment where we have described threat trends in the maritime sector. The threat assessment focuses on terrorism, intelligence, sabotage and other crimes. The analysis is based on trend reports from the NCIS (Kripos), the Police Security Service (PST), and the Intelligence Service (E-tjenesten), as well as FFI research reports and international databases of terrorist incidents. FFI and NKSB also had a conversation with PST on general threat trends in Norway. The KYV headquarters has presented their incident log with various types of threats and security incidents in their sector.

This report recommends that KYV build its risk-based supervision on the ports’ security profile as well as the ports' own conducted vulnerability assessments. The frequency of audits should be considered with regard to both the criticality of the port and experiences from previous audits. The underlying principles of the audit should be broadly known. Thus, it is recommended that the various port facilities are involved in the classification process and in the vulnerability assessments. The report also presents a model for risk-based supervision. The model and the recommendations are based on theoretical contributions from relevant scientific literature and on practical experiences.

Innhold

Forord

Forfatterne retter en stor takk til Andreas Breivik i Kystverket som har bidratt med grunnlagsmateriale, og som har vært en dedikert diskusjonspartner gjennom hele prosessen i utarbeidelse av denne rapporten.

Vi takker også alle representanter fra Kystverkets regionalkontorer som velvillig har stilt opp og gitt oss viktig og klargjørende informasjon gjennom fagdagen i Oslo, samt arbeidsmøter. Takk til PST for konstruktive innspill til den overordnede trusselvurderingen, og til DSB-liaison Maria Due-Hansen som har bidratt med informasjon og tekst om farlige stoffer.

Til sist vil vi takke for alle innspill og tilbakemeldinger vi fikk på et utkast av denne rapporten fra oppdragsgiver og kolleger, samt innspill vi fikk på klassifiseringsmetoden som ble utviklet.

Maren Maal, Kjersti Brattekås, Siw Tynes Johnsen, Janita Bruvoll og Leif D. Riis

Kjeller, desember 2016

1 Innledning

Norge er en langstrakt kystnasjon hvor vi finner havner og havneanlegg i både urbane og rurale strøk. Det å være en kystnasjon gir oss mange muligheter blant annet til å frakte varer via sjøveien både nasjonalt og internasjonalt. Imidlertid kan dette potensielt gjøre oss sårbare ved en situasjon hvor det er et forhøyet trusselnivå. Norge har heldigvis ikke vært utsatt for noen alvorlige terrorhendelser de siste årene, men hendelser i nærliggende land viser at terrortrusselen rammer nasjoner med lignende verdier og styresett som oss. Hvordan vi kan studere, vurdere og håndtere slike hendelser er omdiskutert i både akademia, media og blant politikere. Risikoen for en tilsiktet uønsket handling er kompleks, usikker og tvetydig. Den er heller ikke statisk og vi er dermed helt avhengig av kontinuerlig etterretning for å inneha et reelt og oppdatert trusselbilde.

Den forhøyede terrortrusselen mot Norge sommeren 2014 gjorde at det over hele landet ble iverksatt sikringstiltak. Trusselen var generell og PST hadde ingen indikasjoner på hvor, når og hvem trusselen var rettet mot. For Kystverket, og flere andre virksomheter, ble dette en kostbar affære. På daværende tidspunkt var ikke de ulike havneanleggene klassifisert i sikringsgrupper, og den forhøyede trusselen medførte at sikringsnivået måtte økes ved alle havneanlegg.

Forsvarets forskningsinstitutt (FFI) og Forsvarsbygg futura ved Nasjonalt kompetansesenter for sikring av bygg (NKSB) har på oppdrag fra Kystverket utarbeidet en metode for klassifisering av norske havneanlegg og kommet med anbefalinger til risikobaserte tilsyn. [1]

Denne vurderingen har to overordnede formål. Den skal være "(i) veiledende for det risikobaserte tilsyn KYV fører i norske havner og havneanlegg av deres sikringsregimer, (ii) være veiledende ved fastsettelse av det maritime sikringsnivået i norske havner og havneanlegg, spesielt ved en generell økning av trusselnivået" (Oppdragsavtale mellom FFI og KYV).

Rapporten skal gjennomføre en overordnet trusselvurdering om relevante trusler mot norske havner og havneanlegg.

1.1 Rapportens oppbygging

Rapporten er bygd opp på følgende måte:

Kapittel 2 presenterer bakgrunn og begrepsavklaringer.

Kapittel 3 skisserer FFI og NKSBs forskningsopplegg og hvordan rapportens informasjonsgrunnlag er samlet inn. Det blir referert til grunnlagsdokumentasjonen som har blitt brukt i denne rapporten.

[1] AVTALE mellom KYSTVERKET (KYV) og FORSVARETS FORSKNINGSINSTITUTT (FFI) om Opplegg for trussel- og risikovurderinger av norske havner og havneanlegg.

Kapittel 4 beskriver regelverk og sikringsnivå.

Kapittel 5 gjennomgår generelle trusseltrender og inkluderer en hendelsestabell med de største angrepene mot maritim sektor etter 1980-tallet. Det blir utført en overordnet trusselvurdering som tar for seg de ulike trusselkategoriene, med fokus på maritim terror. Seksjon 5.6 og 5.7 gjennomgår noen anbefalinger og utfordringer knyttet til risikovurderinger for tilsiktede uønskede handlinger, samt hvilke sikringshendelser som bør inkluderes i en risikovurdering.

Kapittel 6 beskriver hvordan en bør klassifisere havneanlegg i Norge. Kapittelet gjennomgår de ulike kriteriene og hvordan FFI og NKSB kom frem til disse. Selve metoden med rangeringstabeller er listet i vedlegg A.

Kapittel 7 beskriver anbefalinger til risikobaserte tilsyn og fastsettelse av det maritime sikringsnivået. FFI og NKSB oppsummerer funnene fra en teoretisk gjennomgang av tilsyn generelt; hvordan ulike tilsynsregimer fungerer; hvordan det har sammenheng med regulering og hvilke utfordringer som kan knyttes til risikobaserte tilsyn. Deretter blir tilsyn forsøkt satt inn en sikringskontekst. Denne teoretiske gjennomgangen er bakgrunn for den videre anbefalingen som blir gitt vedrørende hensyn KYV bør ta i risikobaserte tilsyn. Anbefalingene baserer seg på litteraturstudier og et intervju.

Kapittel 8 oppsummerer rapportens funn og anbefalinger.

1.2 Brukermedvirkning

KYV har deltatt i arbeidet med denne analysen med en rekke personer fra ulike regioner. FFI og NKSBs kontaktperson i KYV har vært Andreas Breivik.

KYV har bidratt med dokumentasjon om virksomheten og bidratt med tilbakemeldinger gjennom flere faglige møter gjennom analyseprosessen. Representantene fra hovedkontoret og regionskontorene var Andreas Breivik, Leif Jansen, Jens Terje Tøraasen, Joakim Flatøy Aae, Helge Digre, Beate Sperre, Tor Hellesen, Kristine Runde Ulstein, Gry Karlsen Lunde, Robin Granås og Sveinung Hustoft.

1.3 Analysegruppen

Analysegruppen består av medarbeidere fra FFI og NKSB med ulik fagbakgrunn, både innenfor risikovurdering og fysisk sikring. Analysegruppen har bestått av følgende personer:

- Kjersti Brattekås (FFI)
- Maren Maal (FFI)
- Janita Bruvoll (FFI)
- Leif D. Riis (NKSB)
- Siw Tynes Johnsen (NKSB)

1.4 Forutsetninger og avgrensninger

Det forutsettes at analysegruppen har fått tilgang til alle etterspurte data og kunnskaper vedrørende virksomheten som berører analysen, som virksomheten har hatt mulighet til å fremskaffe, og at den utleverte dokumentasjonen er oppdatert og gyldig. Analysen er av tidsmessige hensyn kun gjennomført med utvalgte nøkkelpersoner. Analysegruppen mente det var mest hensiktsmessig å gjennomføre en verdivurdering for å besvare spørsmålene som ble skissert av KYV i oppdragsavtalen. Dette fikk analysegruppen støtte for av KYV.

Studien inkluderer følgende avgrensninger: (i) analysen er gjennomført på et overordnet nivå fordi den skal være dekkende for alle ISPS-havneanlegg i Norge, (ii) metoden for klassifisering har havneanlegg som analyseobjekt, (iii) analysen tar høyde for risiko for tilsiktede uønskede handlinger (security), og inkluderer ikke forhold som angår ulykkeshendelser (safety), (iv) det er ikke foretatt vurderinger som angår IKT-sikkerhet eller personellsikkerhet.

2 Bakgrunn og begrepsavklaringer

Denne rapporten utgjør sluttleveransen for oppdraget "Opplegg for trussel- og risikovurderinger av norske havner og havneanlegg". FFI har i samarbeid med KYV og NKSB utarbeidet en klassifiseringsmetode for norske havneanlegg. Rapporten presenterer også anbefalinger til risikobaserte tilsyn.

FFI og NKSB har gjennomført en analyse for å identifisere kriterier som kan brukes i metoden for å klassifisere havneanlegg. Det har blitt tatt utgangspunkt i verdiene, og vi har i så måte gjennomført en verdivurdering. En verdivurdering har som formål å kartlegge virksomhetens verdier, og vurdere hvilke av disse som er viktigst for virksomhetens oppdrag og leveranser. Dette fordrer at man på en systematisk måte vurderer hvilke konsekvenser det kan få dersom verdiene skulle rammes (NSM 2016:11).

I følge Norsk standard 5830 defineres begrepet verdi som "en ressurs som hvis den blir utsatt for uønsket påvirkning vil medføre en negativ konsekvens for den som eier, forvalter eller drar fordel av ressursen" (NS 5830:2012). En trussel defineres som "mulig uønsket handling som kan gi en negativ konsekvens for et havneanleggs sikkerhet" (ibid.). Sårbarhet defineres som "manglende evne til å motstå en uønsket hendelse eller opprette ny stabil tilstand dersom en verdi er utsatt for uønsket påvirkning" (ibid.). Risiko defineres som "forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifikke trusselen" (ibid.).

I følge havneloven defineres fartøy som "enhver flytende innretning som kan brukes som transportmiddel, fremkomstmiddel, løfteinnretning, oppholdssted, produksjonssted eller lagersted, herunder undervannsfartøyer av enhver art". Havn defineres som "områder som er til bruk for fartøy (i) som skal laste eller losse gods eller transportere passasjerer som ledd i sjøtransport eller annen næringsvirksomhet, (ii) har behov for landings- og liggeplasser mv. i forbindelse med utøvelse av fiskeri- og havbruksnæring, (iii) for øvrig har behov for oppankrings- eller liggeplasser eller lignende. Alle områder som hører til eller er funksjonelt knyttet til områder som nevnt i første punkt anses også som havn" (ibid.).

Havnevirksomhet defineres som "tjenesteyting, myndighetsutøvelse og annen offentlig forvaltning som retter seg mot fartøy, gods eller passasjerer i havnen". Havne- og farvannsloven (2009) definerer havneanlegg som "arealer, bygninger, innretninger og annen infrastruktur som brukes i havnevirksomhet, herunder kaier, terminalbygninger, laste-, losse- og omlastningsinnretninger og lager- og administrasjonsbygninger" (Kystverket 2011).

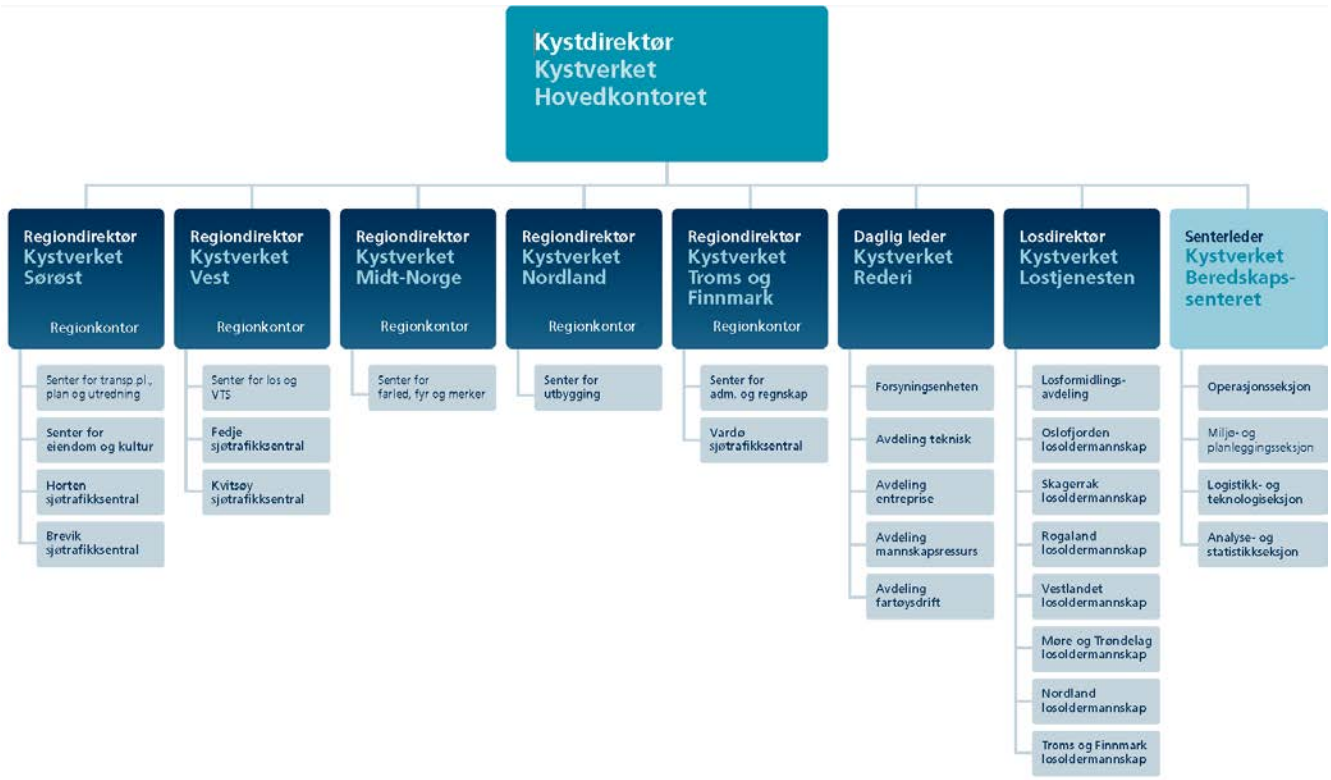
I følge forskrift om sikring av havneanlegg defineres en sikringshendelse som en "en mistenkelig handling eller omstendighet som utgjør en trussel mot et skip, et havneanlegg eller en havn" (Lovdata 2013). Noen steder i rapporten vil sikringshendelser bli omtalt som sikkerhetstruende hendelser, dette brukes kun når analysegruppen viser til definisjoner fra sikkerhetsloven.

Rapporten inneholder en generell del som sier noe spesifikt omkring relevante trusler mot denne næringen. Rapporten foreslår også en klassifisering basert på kritikaliteten til verdien, eller hvor utsatt enkelte havneanlegg vil kunne være for tilsiktede uønskede handlinger. Dette er basert på en verdivurdering, samt kvalitative vurderinger for hver av de ulike rangeringstabellene. Truslene blir kategorisert som terrorisme, etterretning, sabotasje og annen kriminalitet (for eksempel ran og tyveri). Disse trusselkategoriene blir nærmere omtalt i kapittel 5.

Det er ingen entydig definisjon av begrepet risikobasert tilsyn. Dette blir diskutert i mer detalj i kapittel 8.

2.1 Kystverket

Kystverket er en "nasjonal etat for kystforvaltning, sjøsikkerhet og beredskap mot akutt forurensning" og ligger under Samferdselsdepartementet (Kystverket 2016a). Kystverket har ni driftsenheter som inkluderer 5 regioner, rederi, lostjenesten og et beredskapssenter (Kystverket 2016b). Etaten har cirka 50 operative enheter. Kystverket har til sammen 1100 medarbeidere der 700 personer jobber med operativ virksomhet (ibid.).



Figur 2.1 KYV organisasjonskart (Kystverket 2016b)

Kystverkets geografiske virkeområder omfatter "ca. 57 000 km kystlinje (inkludert øyer), 17 fylker, 282 kystkommuner" (Rutledal 2002a). Kystverket har tre hovedmål: (i) Bidra til effektiv sjøtransport, (ii) Sikre trygg ferdsel i norske farvann og havområder, (iii) Hindre / begrense miljøskade som følge av akutt forurensning i norske havområder eller på norsk territorium (Kystverket 2016c). Hovedformålet med Kystverkets virksomhet er å "sørge for best mulig sikkerhet og fremkommelighet for de som ferdes, oppholder seg eller driver næringsvirksomhet i kystsonen, samt å legge alle forhold til rette for at disse kan drive sin virksomhet under best mulige konkurranseforhold og på den mest rasjonelle måte" (Kystverket 2016d). Kystverkets mål for ISPS-arbeidet er at "det skal ikke forekomme terrorhandlinger eller andre sikringshendelser som kan skade norske havner og havneanlegg eller skip som anløper disse"[2].

2.2 Sårbarhetsvurderinger i maritim sektor

Recognized Security Organization (RSO) godkjennes av Kystverket til å gjennomføre *Port Facility Security Assessment* (PFSA) og eventuelt utarbeide *Port Facility Security Plan* (PFSP). Havneanlegget kan også godkjennes som RSO. Sårbarhetsvurderingen (PFSA) gjennomføres av RSO eller av Kystverket, og godkjennes av KYV. PFSA'en skal oppfylle kravene i ISPS-koden, og danner grunnlaget for utarbeidelsen av en sikringsplan. Sårbarhetsvurderingen skal oppdateres minimum hvert 5. år. Denne skal alltid gjennomgås ved endringer i grunnlaget for PFSA, eksempelvis (i) endringer i infrastruktur og eiendeler, (ii) endringer i størrelse og utstrekning, (iii) etablering av ny aktivitet eller virksomhet, eller (iv) endringer i trusler mot havneanlegget. PFSO kan gjennomgå PFSA, men kun gjøre mindre endringer.

PFSP (sikringsplan) kan utarbeides av sikringsleder eller RSO, og den godkjennes av Kystverket. Planen skal bygge på PFSA og skal oppfylle krav i ISPS-koden og forskrift om sikring av havneanlegg kapittel 4. PFSP skal kontinuerlig oppdateres. Den endrede sikringsplanen skal alltid sendes til Kystverket, men endringer som (i) følger av endringer i PFSA og, (ii) som påvirker omfanget av sikringstiltakene, skal godkjennes av Kystverket før de kan iverksettes.

De viktigste sikringstiltakene er at det (i) utarbeides et system som sikrer kontroll med adgangen til havneanlegget og adgangsbegrensede områder og (ii) bagasje, gods m.m. blir gjennomsøkt der formålet er å avdekke ulovlige gjenstander. Havneanlegget kan også benytte seg av stikkprøvekontroll der frekvensen er basert på Kystverkets anbefalinger.

Noen havneanlegg kan få tillatelse til fritak for gjennomføring av noen av kravene i ISPS-koden etter § 11. Hvilke krav besluttes av Kystverket på bakgrunn av PFSA. Havneanlegg som sporadisk betjener skip i internasjonal fart, men i hovedsak nasjonal fart kan få slike fritak. PFSO er den som er utpekt av havneanlegget, har nødvendig kompetanse og er kontaktpunktet til KYV.

[2] Fra arbeidsmøte med KYV 18.10.2016.

3 FFI og NKSBs forskningsopplegg

Det har vært en sentral forutsetning for arbeidet at analysegruppen gjennom hele analysen har hatt god tilgang til fagekspertise hos KYV.

I samråd med KYV la analysegruppen opp til følgende fremgangsmåte for den overordnede vurderingen:

1. Informasjonsinnhenting om sårbarhetsvurderinger innen kyst- og havnesikring gjennom nært samarbeid med KYV, og gjennom fagdagen. Hensikten med dette har vært å få en helhetlig forståelse for sikringsarbeidet knyttet til tilsiktede uønskede handlinger.

2. Analysegruppen bestående av forskere fra FFI og NKSB (seksjon 1.3) har basert seg på opparbeidet systemforståelse gjennom tidligere risikovurderinger for sivile og militære aktører.

3. Analysegruppen har gjennomført en dokumentstudie av faglitteratur, lovverk og andre relevante dokumenter, som for eksempel sårbarhetsvurderinger fra ulike RSO'er.

3. Under arbeidet med kategorisering av havner og havneanlegg har KYV kommet med faglige innspill til analysegruppen.

4. Før ferdigstilling av rapporten har analysegruppen fått innspill fra KYV som har blitt inkorporert i rapporten.

3.1 Forskningsmetode

Denne rapporten har gjennomført en verdivurdering ettersom dette er mest hensiktsmessig med tanke på rapportens overordnede formål (kapittel 1). Å gjennomføre en verdivurdering innebærer å kartlegge virksomhetens verdier, og vurdere hvilke av disse som er viktigst for virksomhetens oppdrag og leveranser. Dette fordrer at man på en systematisk måte vurderer hvilke konsekvenser det kan få dersom verdiene skulle rammes (NSM 2016:11).

For å kunne komme med de mest relevante kriteriene for å klassifisere havneanlegg har analysegruppen vurdert ulike typer kriterier fra sikkerhetsloven og ISPS-kodens del B, 15.5-10. Sikkerhetsloven beskriver at man spesielt skal ta hensyn til verdienes (i) betydning for sikkerhetspolitisk krisehåndtering og forsvar av riket, (ii) betydning for kritiske funksjoner for det sivile samfunn, (iii) symbolverdi og (iv) mulighet for å utgjøre en fare for miljøet eller befolkningens liv og helse. KYV per dags dato ikke er underlagt sikkerhetsloven, men det er noe som kan endre seg når sikkerhetsloven blir oppdatert[3]. For virksomheter som ikke har skjermingsverdige objekter kan man ta utgangspunkt i følgende hovedkategorier; (i) liv og helse: enten for eget personell eller andre personer som benytter eller er avhengige av

[3] Sikkerhetslovutvalget (2016). *Samhandling for sikkerhet*. NOU 2016: 19. Sist besøkt 10.11.2016 https://www.regjeringen.no/no/dokumenter/nou-2016-19/id2515424/sec1

virksomhetens leveranser, (ii) operativ evne eller daglig drift: nedetid for hele virksomheten eller forsinkelser knyttet til viktige leveranser, (iii) informasjon: tap eller kompromittering av sikkerhetsgradert og/eller sensitiv informasjon, (iv) økonomi: kostnader knyttet til erstatning av ødelagt utstyr, skade på bygninger eller nedetid/forsinkelser av viktige leveranser og (v) omdømme: svekket omdømme eller redusert tillit i befolkningen som følge av en sikringshendelse (ISPS-kodens del B, 15.5-10). Den sistnevnte kategorien er ofte nært knyttet til de fire ovenstående, og kan gjerne komme som en konsekvens av disse.

3.2 Dokumentstudier

I dette kapitlet presenteres grunnlagsdokumentasjonen som har blitt brukt i denne rapporten. Det er benyttet et sett med data for å belyse virksomhetens verdier, aktuelle trusselaktører, sårbarheter og andre forhold av sikkerhetsmessig betydning. Dette har blitt gjort tilgjengelig for analysegruppen av oppdragsgiver.

Vi har fått tilgang til sårbarhetsvurderinger utført av "Recognized Security Organisations" (RSO). Vi fikk 24 sårbarhetsvurderinger som dekket havner og havneanlegg fra alle regionene i KYV. Det var dermed god geografisk spredning som var nyttig for arbeidet med denne rapporten. Sårbarhetsvurderingene (PFSA) er i stor grad utført av private konsulentselskaper. Sårbarhetsvurderingene ga oss innsikt i hvilke trusler som blir valgt ut som mest relevant og de ga oss innsikt i diversiteten av havner og havneanlegg.

Rapporten baserer seg på tidligere rapporter fra FFI som gjennomførte en risikovurdering av norsk sjøtransport (Eggereide et al 2007; Rutledal 2002a og Rutledal 2002b), samt en egen rapport som gjennomgikk maritime trusseltrender (Tønnessen 2007). FFI og NKSB fikk også tilgang til en gradert trusselvurdering som var gjennomført av PST i 2013. Dette var nyttig bakgrunnsmaterialet for trusselvurderingen presentert i denne rapporten. Internasjonale kilder og databaser har blitt brukt for å identifisere internasjonale hendelser som var relevante for den generelle trusselvurderingen.

For kapittel 7, som omhandler risikobaserte tilsyn, er det gjort en gjennomgang av relevante fagartikler og -bøker for å få oversikt over feltet. Teoriene er hentet fra flere anerkjente nasjonale og internasjonale forfattere innenfor samfunnssikkerhetsfeltet.

3.3 Fagdag med KYV og workshops

På gjennomførte fagdager ga KYV en innføring i relevante regelverk og dagens rutiner for risikovurderinger og tilsyn. Mer spesifikt handlet dette om "International Ship and Port Facilities Security Code" (ISPS-koden) og andre problemstillinger innen maritim sektor. Fagdagene ble gjennomført med representanter fra hovedkontoret og alle regionskontorene. Det ble også ble det holdt foredrag om hvordan risikovurderinger blir gjennomført av RSO. Ulike sårbarhetsvurderinger fra regionene ble presentert for analysegruppen. KYV orienterte om erfaringer fra heving av maritimt sikringsnivå sommeren 2014.

FFI og NKSB har også hatt mindre møter hvor KYV har kommet med nyttige innspill om sorteringen av ulike havner og havneanlegg i mer finmaskete kategorier. Dette var avgjørende ettersom det er KYV som sitter med fagkunnskapen. De ulike kategoriene av havner ble også sett opp mot ulike typer trusler for å vurdere utsattheten/målattraktiviteten knyttet til ulike typer havner og havneanlegg.

3.4 Semistrukturerte intervjuer

FFI og NKSB har intervjuet personer fra PST og HMS-rådgiver Marit Bjerknes fra FFI som har erfaring med risikobasert tilsyn. Intervjuene ble utført i perioden oktober 2017. Hensikten med å ha samtaler med PST var å kartlegge hva PST anså som de mest relevante truslene mot norske havner og havneanlegg. Hensikten med å intervjue Marit Bjerkes som har erfaring med å utføre tilsyn var å få praktiske erfaringer som kunne supplere vår litteraturstudie som fokuserte mer på teoretiske bidrag.

Respondentene ble først kontaktet på telefon eller epost. Deretter ble et kort informasjonsbrev om formålet med studien samt noen generelle spørsmål oversendt. Intervjuene varte ca. 60 minutter. Respondentene fikk anledning til å se gjennom teksten som henviste til intervjuet før publisering.

4 Regelverk og sikringsnivå

Dette kapittelet gir en oversikt over regelverket for maritim sikring.

4.1 Regelverk

Det er flere lover og regelverk på internasjonalt og nasjonalt nivå som norske havner og havneanlegg må forholde seg til. De mest sentrale internasjonale og nasjonale er som følger:

International Ship & Port Facility Security (ISPS) Code and Safety of Life at Sea (SOLAS) Amendments 2002 kom som et resultat av terrorhendelsene i USA 11. september 2001, og ble vedtatt i *International Maritime Organization* (IMO) i 2002. Formålet med ISPS-koden og tilleggene var å styrke den internasjonale maritime sikringen. ISPS-koden del A, og deler av del B, gjelder som norsk forskrift. Koden gjelder for havneanlegg som betjener følgende skip i internasjonal fart: passasjerskip, lasteskip over 500 BT, flyttbare boreinnretninger og spesialskip (SPS). Alle skip med *International Ship Security Certificate* (ISSC) regnes for å være i internasjonal fart. ISPS-regelverket gjelder ikke for krigsskip, militære hjelpefartøyer, skip i statlig ikke-kommersiell drift, fiskefartøy, skip uten egen fremdriftsmaskineri, primitive treskip og lystfartøy (*pleasure vessels*) (IMO 2003 og IMO 2012).

Regulation (EC) No 725/2004 of the European Parliament and of the Council of March 2004 on enhancing ship and port facility security (EU-forordning 725/2004) har som hovedmål å innføre og iverksette tiltak innenfor EØS med sikte på å bedre sikkerheten for fartøyer som brukes i internasjonal handel og nasjonal skipsfart, samt tilhørende havneanlegg, mot trusselen fra forsettlig ulovlige handlinger. Den slår fast at sikkerheten til skipsfarten til enhver tid må sikres mot trusler om forsettlig ulovlige handlinger som terrorhandlinger. EU-forordningen presiser imidlertid at for havneanlegg som ligger i havner som bare leilighetsvis betjener internasjonal skipsfart kan det være en uforholdsmessig stor oppgave å følge alle sikkerhetsreglene som er fastsatt, og at dette skal vurderes av statene selv (EU 2004).

Directive 2005/65/EC of the European Parliament and of the Council on 26 October 2005 in enhancing port security (EU-direktiv 2005/65) har som hovedformål å øke havnesikringen overfor sikkerhetshendelser, i tillegg til å sørge for at sikringstiltakene fra EU-forordning 725/2004 drar nytte av økt havnesikring. Direktivet fremhever behovet for detaljerte sikkerhetsvurderinger som avgrenser havneområdet og beskriver sikringstiltak. Tiltakene bør variere med sikkerhetsnivået som er etablert og reflektere de ulike risikoprofilene til ulike deler av et havneområde. Medlemsstatene skal godkjenne vurderinger og planer, og sørge for implementeringen av disse i egne havner (EU 2005).

Commission Regulation (EC) No 324/2008 of 9. April 2008 laying down revised procedures for conducting Commission inspections in the field of maritime security (EU-forordning 324/2008) beskriver prosedyrene for kommisjonens gjennomføring av inspeksjoner av

implementeringen av EU-forordning 725/2004 og EU-direktiv 2005/65 på medlemsstatsnivå og i de enkelte havner (EU 2008).

Når det gjelder norsk regelverk har FFI og NKSB studert følgende:

Lov om havner og farvann (2009) har som formål å legge til rette for god fremkommelighet, trygg ferdsel og forsvarlig bruk og forvaltning av farvannet. Videre skal loven legge til rette for effektiv og sikker havnevirksomhet som ledd i sjøtransport og kombinerte transporter, samt for effektiv og konkurransedyktig sjøtransport av personer og gods innenfor nasjonale og internasjonale transportnettverk. Loven fremhever at departementet kan gi forskrifter om sikkerhets- og terrorberedskapen i havner og havneterminaler. Dette inkluderer bl.a. plikten til å foreta en sårbarhetsvurdering, til å ha en godkjent sikkerhets- og terrorberedskapsplan og adgang til å foreta kontroll av personer, kjøretøy og gjenstander som er eller skal inn i havn eller havneterminal. Lovens § 43, som omhandler sikkerhet og terrorberedskap, er ikke utdypet videre i Kystverkets veiledning om havne- og farvannsloven (Samferdselsdepartementet 2009 og Kystverket 2011).

Lov om losordningen (Losloven 2014) skal legge til rette for en losordning som skal bidra til å trygge ferdselen på sjøen ut fra samfunnsmessige hensyn. Loven skal videre medvirke til at Forsvaret kan løse sine oppgaver. Loven gjelder i sjøterritoriet og i de indre farvann såfremt annet ikke er bestemt i loven (Samferdselsdepartementet 2014). Kystverkets oppgaver etter Losloven inkluderer tilsyn med at regler gitt i medhold av loven følges, i tillegg til losformidling, organisering av lostjenesten, sertifikatkontroll og farledsbevisordningen (Kystverket 2011).

I 2013 ble to nye forskrifter introdusert, og formålet med forskriftsrevisjonen var å lage et regelverk som er mer fleksibelt og bedre tilpasset ulikhetene i norske havner, samt å gjennomføre det internasjonale regelverket på en korrekt måte. **Forskrift om sikring av havneanlegg (2013)** og **Forskrift om sikring av havner (2013)** skal være komplementære, og har som hovedformål å forebygge og hindre sikringshendelser som kan skade havner, havneanlegg eller skip som anløper disse. Disse forskriftene erstatter følgende utgåtte forskrifter: Forskrift om sikkerhet og terrorberedskap i norske havner (2004), Forskrift om sikring av havner og havneterminaler mot terrorhandlinger mv. (2007), og Forskrift om gebyr for kontroll og tilsyn med sikring av havner og havneterminaler mot terrorhandlinger mv. (2007). I de nye forskriftene er det mer fokus på mål enn middel – man har gått bort fra de detaljerte minimumskravene, og over til å, i større grad, benytte seg av funksjonskrav. Det legges mer vekt på sårbarhetsvurderingen, det har blitt innført krav til opplæring for PFSO og PSO, og krav til både kursinnhold og kursholdere. Det er også gjennomført noen begrepsendringer, blant annet for begrepet havn, som her defineres som "et bestemt land- og sjøområde med grenser fastsatt på bakgrunn av en sårbarhetsvurdering, og som inneholder anlegg og utstyr som benyttes til å betjene kommersiell sjøtransport. Med havnens grenser menes her grensene for det sikringsrelevante havneområdet" (Samferdselsdepartementet 2013a og 2013b).

I tillegg til lover og forskrifter som går direkte på havner og havneanlegg, har FFI og NKSB i tillegg studert **Lov om forebyggende sikkerhetstjeneste** (sikkerhetsloven 1998), og tilhørende forskrifter. Sikkerhetslovens formål er å legge forholdene til rette for effektivt å kunne motvirke trusler mot rikets selvstendighet, sikkerhet og andre vitale nasjonale sikkerhetsinteresser, og den gjelder for alle statlige og kommunale organene i Norge. Loven definerer blant annet sikkerhetstruende hendelser som spionasje, sabotasje og terrorhandlinger (Forsvarsdepartementet 1998).

4.2 Maritimt sikringsnivå

ISPS-koden beskriver tre nivåer av maritim sikring, og disse er i bruk internasjonalt. Begrepet *sikringsnivå* viser her til risikoen for at en sikringshendelse skal skje eller bli forsøkt gjennomført. Disse sikringsnivåene benyttes også i Norge, og det er KYV som beslutter endring i nivå for havner og havneanlegg. Etter at dette besluttes sendes det ut melding om nivåendring til PSO/PFSO, som så umiddelbart skal iverksette sikringstiltak.

Sikringsnivå 1 er normalnivå, og innebærer et minstekrav til relevante sikringstiltak som skal implementeres og håndheves til enhver tid. Dette kan sammenstilles med det som i henhold til sikkerhetslovens begrepsbruk omtales som *grunnsikring*. Hensikten er at dette sikringsnivået skal kunne håndtere de vanligste formene for kriminalitet i tilknytning til havner og skip, som uautorisert adgang på området, simpelt tyveri og blindpassasjerer. Sikringsnivå 2 er gjeldende ved økt risiko for en sikringshendelse. Da må man sette inn ekstra sikringstiltak i forhold til normalnivået, for å kunne opprettholde fortsatt kommersiell drift av havnen. Sikringsnivå 3 betyr at en sikringshendelse er sannsynlig eller umiddelbart forestående. Da må man implementere ytterligere sikringstiltak. Skip som anløper havnen skal ikke ha lavere sikringsnivå enn havneanlegget. Typiske sikringstiltak innebærer inngjerding, overvåkning, adgangskontroll, kontroll med last og skipsforsyninger samt andre beredskapstiltak.

ISPS-koden fremhever at man kun bør sette sikringsnivå 3 i spesielle omstendigheter. Man må vurdere informasjonen man har om en ventet sikringshendelse basert på hvorvidt den er troverdig, bekreftet, umiddelbar og spesifikk, samt de potensielle konsekvensene sikringshendelsen vil kunne medføre. Nivå 3 bør også tidsbegrenses basert på informasjonen man har tilgjengelig. Myndighetene kan velge å sette det samme sikringsnivået for alle havner og havneanlegg, eller å differensiere mellom ulike typer havner, havneanlegg eller skip (IMO 2012: 34-36).

5 Overordnet trusselvurdering

I denne overordnede trusselvurderingen er begrepet trussel knyttet til hendelser som kan inntreffe og som er gjennomført med hensikt, for å påføre skade. Det dreier seg altså om tilsiktede uønskede handlinger, ikke ulykker, naturkatastrofer og tekniske feil.

I denne kartleggingen er det lagt vekt på å identifisere mulige trusler innenfor kategoriene terror, etterretning, sabotasje og annen kriminalitet. Dette samsvarer med sikkerhetslovens definisjon av sikkerhetstruende virksomhet. Det er ikke noe klart skille mellom disse begrepene. Det er like mye aktørens hensikt med handlingen som selve handlingen som avgjør hvilken betegnelse som brukes.

Ettersom analysegruppen har vektlagt trusler mot havner og havneanlegg i norsk kontekst har vi valgt å ikke ta med piratvirksomhet. Vi henviser kun kort til trusler som smugling, bombetrusler og blindpassasjerer. Dette er fordi vi fant lite informasjon om dette i litteraturen og dermed baserer oss hovedsakelig på KYV sin oversikt over registrerte hendelser.

Kartleggingen av trusler er basert på rapporter fra PST, FFI, Etterretningstjenesten, Kripos, informasjon fra åpne mediekilder og en samtale med PST.

5.1 Oversikt over trusler

Maritim sektor har historisk sett ikke vært et attraktivt mål for terroranslag. I følge RAND[4] sin terrorismedatabase har terroranslag mot maritime mål (hovedsakelig skip) kun utgjort 2 prosent av alle internasjonale terrorhendelser i løpet av de siste 30 årene (RAND 2006 og Nincic 2012).

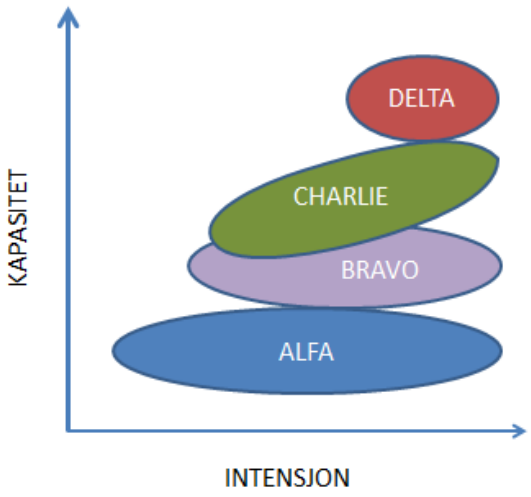
Det siste store maritime angrepet var bombingen av M/V Limburg nær Jemen i 2002. Siden da har maritime angrep vært mindre, og i stor grad bestått av bombeangrep i nærheten av havneanlegg eller mistenkelig aktivitet som involverer lektere (Nincic 2012).

I Norge har det vært svært få, om noen, terroranslag mot sjøtransport eller havneanlegg (Tønnessen 2007). Imidlertid har det vært meldt inn flere sikringshendelser, som blant annet menneskesmugling, blindpassasjerer og bombetrusler.[5] KYV har siden 2014 registrert sikringshendelser i norske havner og havneanlegg. Det er hovedsakelig fire typer av sikringshendelser som har blitt registrert: (1) forsøk på inntrenging til et avgrenset område, (2) blindpassasjerer, (3) tyveri, og (4) mistenkt etterretningsaktivitet i havneområdet. Blindpassasjerer er, ifølge KYV, den typen tilfeller som skjer oftest i norske havner og havneanlegg.

[4] RAND har en internasjonal database med statistikk over terrorhendelser.
[5] Basert på samtaler og møter med KYVs hovedkontor.

Det er flere hendelser i og utenfor Norge som påvirker sikringsarbeidet for maritime virksomheter. Hendelser i andre land og andre sektorer vil kunne påvirke både trusselbilde og sikringsarbeidet i maritim sektor. Hendelsene 22. juli 2011 og angrepet i In Amenas har vist at terrorangrep både kan skje her hjemme, samt at de kan ramme norske interesser i utlandet. Rapportene etter disse hendelsene har også vist at det er flere mangler i måten sikringsarbeidet ble utført på, og det økte fokuset på dette vil trolig lede til endringer i flere sektorer enn de som ble berørt. Den maritime sektoren er også styrt av et internasjonalt lovverk, som videre vil si at store internasjonale hendelser vil kunne påvirke gjeldende lover og krav til sikkerhet. Eksempelvis førte 9/11 til en rask omveltende opptrapping av flyplassikkerhet over hele verden, for maritim sektor førte hendelsen til at ISPS-regelverket ble introdusert.

Sikringshåndboka deler trusselaktørers intensjon og kapasitet inn i fire forskjellige nivåer, ALFA, BRAVO, CHARLIE og DELTA. ALFA er det laveste nivået, og kjennetegnes av personer med liten eller ingen kriminell erfaring. DELTA er det høyeste nivået, og kjennetegnes av militære spesialstyrker med tilgang til alle "*state of the art*" verktøy og våpen. Nivåene i mellom, BRAVO og CHARLIE, er noe mer glidende i overgangene og rommer mer erfarne og organiserte kriminelle og ulike typer terrorister (Forsvarsbygg 2016).



Figur 5.1 Nivåer for trusselaktører, basert på aktørenes kapasitet og intensjon.

I trusselvurderinger for enkelte havner/havneanlegg bruker man ofte parameterne (i) *tilstedeværelse* (er det noen her som kan gjøre det?), (ii) *kapasitet* (er den som er til stede i stand til å gjøre det?), (iii) *intensjon* (har vedkommende vilje til å gjøre det?), (iv) *historie* (har det skjedd tidligere?), og (v) *målvalg* (er det noe som tyder på at det kan skje snart?). Samtidig må det understrekes at FFI og NKSB mener at man må ha en verdisentrisk tilnærming til sikring. Dette innebærer at man tar utgangspunkt i hvilke verdier som skal beskyttes og at det på bakgrunn av verdienes kritikalitet, potensielle trusler og sårbarheter, etableres en grunnsikring som skal kunne motstå trusler i en normalsituasjon. For å kunne håndtere endringer i

trusselbildet er det viktig at virksomheten har et beredskapssystem som kan iverksettes på kort varsel slik at sikkerhetsnivået står imot den økte trusselen. Denne tilnærmingen støtter PST.

5.2 Terror

Terrorhandlinger defineres i sikkerhetsloven (Lovdata 2008) som "ulovlig bruk av, eller trussel om bruk av, makt eller vold mot personer eller eiendom, i et forsøk på å legge press på landets myndigheter eller befolkning eller samfunnet for øvrig for å oppnå politiske, religiøse eller ideologiske mål". Maritim terror blir definert som "gjennomføring av terrorhandlinger og aktiviteter (1) innenfor det maritime miljøet, (2) med eller mot fartøyer eller faste plattformer til sjøs eller i havn, eller mot noen av passasjerene eller personell, (3) mot kystanlegg eller nærliggende bygninger, inkludert turiststeder, havneområder og havnebyer eller byer" (Council for Security Cooperation in the Asia Pacific sitert i RAND 2006).

Nesser et al. (2016:10) understreker at Europa står overfor en økende trussel fra jihadister. Det har aldri vært et høyere antall angrepsplot per år enn i perioden 2014-2016. Mellom 2014-2016 har 273 personer blitt drept av jihadistisk vold i Vest-Europa (ibid). Dette skyldes et lite antall svært dødelige hendelser: (i) angrepene i Paris den 13. november 2015 der 130 personer ble drept, (ii) angrepene i Brussel 22.mars 2016 der 32 personer ble drept, og (iii) lastebilangrepet i Nice der 84 personer ble drept (ibid).

FFIs forskning viser at bruk av bomber og skytevåpen har vært, og kommer sannsynligvis til å være, den mest brukte aksjonsformen innenfor jihadistisk terrorisme også i de neste tre-fem årene (Nesser og Stenersen 2014:3). Det fremheves at stadig flere aksjoner gjennomføres med våpen som både er enklere å få fatt i og enklere å bruke enn for eksempel eksplosiver. FFI beskriver at i perioden 2001-2007 forekom kniver og skytevåpen i kun 12 prosent av de identifiserte planlagte og gjennomførte terrorplottene, mens man etter 2008 ser dem i 40 prosent av tilfellene (Stenersen og Nesser 2014). Nesser et al. (2016:10) bekrefter denne trenden og påpeker at skytevåpen har blitt mer vanlig enn eksplosiver. Samtidig blir det presisert at hendelsene fra 2014-2016 tegner et svært komplekst trusselbilde. Valg av våpen og taktikk blir mer diversifisert og målutvelgelsen er mer uklar (ibid).

Europol (2016) har gjennomgått de siste terrorhendelsene i Europa og påpeker at det har vært en endring i modus operandi hos den Islamske Stat (IS). Europol (2016:3) påpeker på bakgrunn av hendelsene i Paris (november 2016) og Brussel (mars 2016) at angrepene har blitt mer komplekse og koordinerte, og at terrorplottene blir gjennomført av grupper. Nesser et al (2016:10) advarer mot å generalisere på grunnlag av noen få og nylige hendelser. De viser bl.a. til at 50 % av alle terrorplott blir gjennomført av enkeltpersoner (Nesser et al 2016:13).

Tønnessen (2007:7) argumenterer at "trenden når det gjelder maritime terroranslag, som for terrorisme forøvrig, går mot enklere, men samtidig mer dødelige angrep". Dette samsvarer med Asal og Hastings (2014), som hevder at terrorgrupper er relativt konservative i valg av strategi og modus operandi. Å angripe et mål til sjøs er ofte utenfor tradisjonelle terrorgruppers kompetanseområde, ettersom det kan kreve mer opplæring og behov for annet materiell. Å

planlegge et angrep på land, som for eksempel involverer en bilbombe, en selvmordsvest, eller et bakholdsangrep med håndholdte våpen, har lenge vært en del av terrorgruppenes repertoar. Denne type modus operandi er ofte en del av en standardopplæring i terrorgrupper. Det å angripe maritime mål, som skip, krever imidlertid ressurser som båter, store mengder drivstoff (spesielt hvis målet er langt fra land), muligens sjødyktig kommunikasjon, navigasjonsutstyr og trening. Det er ikke nødvendigvis allment kjent blant tradisjonelle terrorgrupper hvordan man skal bruke maritime navigasjonssystemer og gjennomføre skipsoperasjoner. Dette kan tolkes som noen av grunnene til at det har vært få hendelser knyttet til terroranslag mot fartøy (RAND 2006).

Havner, havneanlegg og skip som transporterer større grupper mennesker er et attraktivt mål for terrorister ettersom dette innebærer store ansamlinger av mennesker. Internasjonal cruisetrafikk blir trukket frem som det mest "attraktive målet for terrorister, samtidig som det er vanskelig å angripe cruisetrafikken på grunn av høy sikkerhet" (RAND 2006). Tønnessen (2007:7) påpeker at passasjerferjer dermed er mer utsatt "ettersom sikkerheten her er noe lavere og det er mindre ressurskrevende å gjennomføre terrorhandlinger".

Når det gjelder trusler mot norsk sjøfart og norske havneanlegg er det verdt å merke seg at PST i den ugraderte trusselvurderingen for 2016 sier at "ekstrem islamisme vurderes fortsatt å utgjøre den største terrortrusselen, og det er mulig at det i løpet av 2016 vil bli forsøkt gjennomført terrorangrep i Norge" (PST 2016:4). Det må presiseres at PST har ikke spesifikt vurdert sannsynlighet for terroranslag mot havneanlegg. I lys av litteraturgjennomgangen ovenfor er det tydelig at havneanlegg med passasjertrafikk (cruise- og fergetrafikk) er mer utsatt for anslag fra terrorister enn havneanlegg som ikke har passasjerer.

FFI og NKSB har utarbeidet en hendelsestabell med utvalgte hendelser fra 1980 frem til 2016. Gjennom dokumentstudier og samtaler med KYV ble noen hendelser valgt ut. I tabellen er det en kort beskrivelse av hendelsen samt modus operandi. Det er viktig å påpeke at denne hendelsestabellen ikke er utfyllende og at den baserer seg på sekundærlitteratur som i hovedsak omtaler internasjonale hendelser.

Oversikt over utvalgte hendelser innenfor maritim terrorisme	
1985, Egypt	En italiensk cruisebåt "Achille Lauro" ble angrepet av *Palestinian Liberation Front (PLF)* rett utenfor kysten av Egypt. Cruisebåten ble kapret og terroristene tok 511 passasjerer som gisler. Kravet fra PLF var løslatelse av palestinske fanger i Israel. En amerikaner ble drept under denne hendelsen. Det ble brukt skytevåpen (Kalashnikov), granater og eksplosiver (Global Terrorism Database 2015a).
2000, Adenbukta	I 2000 ble en liten båt med selvmordsbombere lastet med sprengstoff detonert i skipssiden på en US Navy destroyer "U.S.S. Cole". Selvmordsbomberne hadde eksplosivene (dynamitten) på kroppen. Hullet i skipssiden var på størrelsen med et hus. U.S.S Cole hadde stoppet for å tanke drivstoff i havnen i Aden, Jemen. Sytten amerikanske sjømenn ble drept og 35 andre ble skadet i eksplosjonen. Al-Qaida stod bak angrepet (Global Terrorism Database 2015b).
2002, Adenbukta	I 2002 ble en jolle lastet med eksplosiver (TNT sprengstoff) detonert mot skipssiden til den franske oljetankeren MV Limburg. Ett besetningsmedlem på MV Limburg ble drept og tolv andre ble skadet. Oljetankeren tok fyr og det lakk ut 90.000 fat olje i Adenbukta. Al Qaida har senere tatt ansvaret for angrepet på nettstedet Jihad.net, som nå er lagt ned (Global Terrorism Database 2015c). Mange av de samme personene som var innblandet i angrepet på USS Cole ble antatt å være involvert i dette angrepet. Adan Abyan Islamic Army (AAIA) sto bak angrepet. I tillegg til de umiddelbare skadene på oljetankeren, ble all frakt til Adenbukta stanset. Dette kostet regjeringen i Jemen ca. 3,8 millioner USD dollar tap per måned (ibid.).
2004, Filippinene	I 2004 ble 20 dynamittkubber gjemt i et uthult tv-apparat som ble fraktet med et Abu Sayyaf-medlem om bord i en ferge i Manila, Filippinene. Fergen het Superferry 14. Bomben forårsaket en kraftig eksplosjon og utløste en brann som raskt spredte seg over hele skipet på grunn av et ineffektivt sprinkleranlegg på fergen. Bomben gikk av ved hjelp av et tidsur omtrent en time etter at den seilte fra Manila. Ombord i fergen var det 899 passasjerer og mannskap. 116 personer ble drept under angrepet. Abu Sayyafs talsmann Abu Soliman og leder Khaddafy Janjalani tok på seg ansvaret for angrepet. Hendelsen har blitt oppført som den mest ødeleggende terrorhandlingen i maritim historie og den fjerde mest alvorlige internasjonale hendelsen etter 11. september 2001 (Rand 2006:22).

Terrorgrupper som har angrepet maritim sektor
Liberation Tigers of Tamil Eelam (også kalt Tamiltigrene): Tamiltigrene har vært aktive de siste årene og vært kjent for å angripe skip utenfor kysten av Sri Lanka. Deres primære mål har vært srilankiske marineskip, men de har også vært involvert i å angripe kinesiske og nordkoreanske skip. Hensikten var å forstyrre skipstrafikk i regionen. De har skilt seg ut fra andre terroristgrupper som har angrepet maritime mål ved at deres modus operandi ofte inkluderer selvmord som en del av angrepsformen (Bakir 2007:7-8).
Tsjetsjenske opprørere: I 1996 kapret Tsjetsjenske opprørere en ferge som seilte fra en nordlig havn i Tyrkia (Trabzon). De krevde en tilbaketrekking av russiske tropper fra en daghestanisk landsby. Etter en rekke forhandlinger, ble kaprerne senere tatt til fange (Bakir 2007:7-8).
Hizbollah: Hizbollah har vært mindre kjent for sine angrep i det maritime domenet. På midten av 80-tallet var de imidlertid aktive i å legge miner i Rødehavet for å hindre tilgang til israelske havner. I 1984 utførte de et mineangrep ved den sørlige inngangen til Suezkanalen som rammet 19 skip (Bakir 2007:7-8).

Tabell 5.1 Oversikt over utvalgte hendelser fra 1980 frem til 2016 innenfor maritim terrorisme. Hendelsestabellen er basert på sekundærlitteratur og er ikke en utfyllende tabell.

5.3 Etterretning/spionasje

Spionasje er i sikkerhetsloven definert som "innsamling av informasjon ved hjelp av fordekte midler i etterretningsmessig hensikt". Etterretningstrusselen mot norske interesser er vurdert av PST til å være "betydelig", og tjenesten oppfordrer til "målrettet innsats for å beskytte sikkerhetsgradert og annen sensitiv informasjon". NSM har fulgt opp med å vise til erfaring som tilsier at "flere virksomheter ikke i tilstrekkelig grad tar hensyn til at etterretningstrusselen er betydelig" (Elgsaas og Heireng 2014).

Det er kanskje mest vanlig å tenke på etterretning i sammenheng med fremmede makter som ønsker å tilegne seg informasjon om en stats nasjonale anliggende, men etterretningstrusselen kan også komme innenfra virksomheten selv. Det er registrert få hendelser knyttet til utro tjenere i Norge, men de dekker et bredt spekter av virksomheter. Politiet peker på at utro tjenere i offentlig sektor kan være en aktuell problemstilling. Det finnes også eksempler på at kriminelle aktører aktivt søker kontakt med personer som i kraft av sin stilling kan være nyttige (Kripos 2014). Motivene til innsidere kan variere, og innsidere har vanligvis mer enn bare ett motiv, men primærmotivene fordeler seg henholdsvis mellom økonomisk vinning (47 prosent), ideologi (20 prosent), ønske om anerkjennelse (14 prosent) og lojalitet (14 prosent) (CPNI 2013). [6]

[6] For mer informasjon om utro tjener-problematikk se veilederen til CPNI (2013) *"Personnel Security Risk Assessment"*.

PST påpeker i sin åpne trusselvurdering av 2016 at etterretningstrusselen i og mot Norge er høy (PST 2016). I møte med PST ble det formulert at flere fremmede staters etterretningstjenester er representert i Norge, men PST vurderer at etterretningstrusselen fra Russland utgjør det største skadepotensiale for Norge og norske interesser. Russiske etterretningstjenesters oppdrag er blant annet styrt av langsiktige russiske sikkerhetsinteresser. Forsvars, sikkerhets- og beredskapsmessige forhold i Norge samt militær og sivil infrastruktur er etterretningsmål for disse tjenestene. PST vurderer det slik at formålet med virksomheten er å legge til rette for russiske militære disposisjoner i en eventuell endret fremtidig sikkerhetspolitisk situasjon. Norges infrastruktur, herunder norske havner, er mål for enkelte fremmede staters etterretningstjenester. Havneanlegg med en strategisk viktig plassering, som har en rolle i vår militære beredskap eller som er knyttet til norsk petroleumsvirksomhet er spesielt utsatt, både med tanke på mulig sabotasjeplanlegging og militærtaktisk bruk ved en eventuell fremtidig sikkerhetspolitisk krise. Resultatet av slik etterretningsaktivitet vil, i ytterste konsekvens, kunne true Norges territorielle kontroll og sentrale samfunnsinteresser.

Etterretningsaktiviteter gjennomføres i utgangspunktet med den hensikt å få tak i informasjon. Etterretning kan også være en forberedelse til gjennomføring av kriminelle handlinger, sabotasje eller terroraksjoner. Det antas at aktører vil utføre en viss form for rekognosering, kartlegging eller etterretning før slike handlinger utføres (Forsvarsbygg 2005). Det er denne typen etterretning, som utføres i forkant av andre typer sikkerhetstruende hendelser, som analysegruppen tror har mest relevans for norske havneanlegg. Dette inkluderer alt fra forholdsvis enkel fysisk rekognosering på området til forsøk på å få tak i sensitive planverk og tekniske tegninger, samt kartlegging av hvordan man kan sabotere eksisterende sikringstiltak i forbindelse med militær sabotasje (Forsvarsbygg 2005).

5.4 Sabotasje

Sabotasje er i sikkerhetsloven definert som “tilsiktet ødeleggelse, lammelse eller driftsstopp av utstyr, materiell, anlegg eller aktivitet, eller tilsiktet uskadeliggjøring av personer, utført av eller for en fremmed stat, organisasjon eller gruppering.”

Sabotasje utført av en fremmed makt anses som svært uvanlig under fredsmessige forhold, og vil normalt bli gjennomført i forkant av en svært alvorlig krise/krigssituasjon (Forsvarsbygg 2005). Mens det anses som mindre sannsynlig at transportsystemer blir utsatt for velplanlagte og omfattende sabotasjeaksjoner i fredstid, finnes det flere typer aktører som kan gjennomføre mindre omfattende aksjoner som kan føre til svikt. FFI fremhever sabotasje gjennomført i forbindelse med annen kriminell virksomhet og sabotasje gjennomført av enkeltindivider med generell destruksjonstrang eller utro tjenere som eksempler på dette. Disse formene for sabotasje vil naturlig nok ikke være hendelser av samme omfang og intensitet som et militært angrep, men konsekvensene kan bli alvorlige nok når de gjennomføres på riktig sted (Friedheim et al. 2009).

PST trekker også frem at "trusselen fra de høyreekstreme miljøene i Norge er vurdert som økende" og at dette kan føre til en økt sannsynlighet for voldshandlinger og sabotasje (PST 2016). Det vurderes som mer trolig at høyreekstreme vil ha asylmottak som mål for en sabotasjeaksjon, enn havneanlegg og sjøtransport.

5.5 Annen kriminalitet

Kriminalitet er handlinger som er straffbare i henhold til Straffeloven, og utviklingen innenfor kriminalitet følger samfunnsutviklingen som sådan. Dette innebærer at man får økt transnasjonal mobilitet og globalisering også innenfor kriminelle miljøer. Man ser at registrert vinningskriminalitet i Norge har gått betraktelig ned de siste årene, i likhet med i de fleste andre vestlige stater. Det som derimot er verdt å merke seg, er at Norge med sin rikdom står i sterk kontrast til de fleste andre landene i Europa, og på den måten representerer norske verdier attraktive mål for utenlandske vinningskriminelle (Kripos 2014).

Organisert kriminalitet defineres i Sikringshåndboka som kriminelle handlinger som utføres av kriminelle grupper eller nettverk som samarbeider, med en form for ledelse, og som over tid opererer med kriminelle handlinger som eneste eller som en dominerende inntektskilde (Forsvarsbygg 2005). Kripos påpeker at kriminalitetsutfordringer innenfor feltet organisert kriminalitet bærer preg av at kriminelle aktører benytter seg av spesiell kompetanse og/eller kunnskap i sine aktiviteter. Dette kan tyde på at man i dag ser en utvikling mot økende profesjonalisering blant aktørene, der man arbeider målrettet og rasjonelt for å maksimere utbyttet av kriminelle handlinger, spesielt når man ser dette i sammenheng med nedgangen i registrert vinningskriminalitet (Kripos 2014).

Mens både sabotasje og terrorangrep er uvanlige hendelser i norsk maritim sjøfart, forekommer trusler om slike angrep oftere (for eksempel bombetrusselen i Tananger i 2012). Bombetrusler kommer ofte fra psykisk ustabile personer eller personer i en fortvilet livssituasjon, som verken innehar nødvendig kompetanse eller kapasitet til å gjennomføre aksjoner med eksplosiver. Det bør imidlertid nevnes at man ikke skal ta lett på bombetrusler, da det i ytterste konsekvens vil kunne påvirke liv og helse dersom trusselen materialiseres.

5.6 Hvilke scenarioer bør RSO'er inkludere i egne analyser?

De siste årene har en vært vitne til flere terrorhendelser i Europa. Spørsmålet er om dette er aktuelt for norske havneanlegg basert på de verdiene som skal beskyttes. PSTs åpne trusselvurdering for 2016 vurderer ikke hvorvidt angrep mot norske havneanlegg og sjøtransport anses som attraktive mål i norske, ekstremistiske miljøer. Samtidig må det understrekes at havneanlegg som har betydelige folkemengder grunnet cruise- og fergetrafikk er mer utsatt enn havneanlegg som ikke har passasjerer. Havneanlegg med cruise- og passasjertrafikk bør ha med terrorscenarioer i sine analyser. Havneanlegg som er viktige for Forsvaret eller som er knyttet til norsk petroleumsvirksomhet bør ha med scenarioer som tar for seg etterretningstrusselen.

Det anbefales å følge KYV sin veileder slik at man får en systematisk tilnærming til sårbarhetsvurderingen. Når det gjelder trusselvurderingen er det viktig å lese PST sin åpne trusselvurdering og Etterretningstjenestens FOKUS. I PSTs årlige åpne trusselvurdering peker de ut hva som kan være generelle mål for ulike trusselaktører. Det er viktig å vurdere om havneanlegget du vurderer passer med målene som PST har identifisert. Dersom det er en hendelse som fører til økt trusselnivå må man basere seg på informasjon fra myndighetene.

Et annet relevant scenario som RSO'er bør ta høyde for er trusselen som en utro tjener/innsider kan utgjøre. Dette er særlig viktig for havneanlegg som har mange operatører og utbredt konsulentvirksomhet.

5.7 Sårbarhets- og risikovurderinger for tilsiktede uønskede handlinger

Det er bred akademisk enighet om at det er tilknyttet stor usikkerhet til security-relaterte risikoer, og da særlig til terrorismerisikoen (Aven 2015; Fishhoff 2002; Renn 2008; Jore og Njå 2012; Weiss 2007; DSB 2014; NSM 2016; Busmundrud et al 2015). Dette vil ha betydning for risikoanalyser og -vurderinger hvor disse risikoene inngår. Den tradisjonelle måten å vurdere risiko der parameterne sannsynlighet og konsekvens gir en estimert, gjerne kvantitativ risikoskåre, kan for security-relaterte hendelser sies å være mindre hensiktsmessig (Jore og Njå 2010; Aven et al. 2004; Renn 2008 og Pettersen og Engen 2010). En slik tilnærming er utfordrende når en skal fange opp usikkerheten knyttet til tilsiktede uønskede handlinger. Dette er fordi en mangler meningsfull statistikk over tidligere hendelser, dermed blir en frekventistisk framstilling av risiko feilaktig. For å fange opp usikkerhetsdimensjonen er det viktig å ha en tilnærming til risiko som erkjenner at risikovurderinger er subjektive, og ikke resulterer i objektive kvantifiserbare fakta. Dette vil for eksempel være gjeldende for risikovurderinger for ulike havneanlegg i Norge. Selv om selve trusselen kan være den samme kan man vurdere sårbarhetene og verdiene annerledes. Variasjoner i intensjon, kapasitet, motivasjon og mål kan også være svært varierende på ulike lokasjoner i Norge. En vurdering av bakgrunnskunnskapen som analytikeren besitter på gitt tidspunkt vil derfor være nødvendig for å kunne si noe om den faktiske risikoen, og tydeliggjøre usikkerheten knyttet til vurderingene.

6 Klassifisering av havneanlegg i Norge

Det å kategorisere alle norske havneanlegg er svært krevende. Det å gruppere alle de ulike havneanleggene i Norge er komplekst ettersom havneanleggene er svært forskjellig. Det er en balansegang mellom altfor grove kategorier og for detaljerte finmaskete kategorier. Med innspill fra KYVs hovedkontor ble det utarbeidet noen overordnede kategorier for havneanlegg.[7] Etter innspill fra regionskontorene og hovedkontoret kom det frem at disse kategoriene ble for grove. Dermed har analysegruppen bestemt seg for at det er mest formålstjenlig at havneanleggene selv vurderer hvilken sikringsprofil de ender opp i basert på den metodiske tilnærmingen skissert i kapittel 7, og beskrevet i vedlegg A.

FFI og NKSB anbefaler at havneanleggene selv gjennomfører denne vurderingen, deretter kan KYV se gjennom vurderingen og kvalitetssikre. Basert på denne klassifiseringen kan KYV identifisere noen fellestrekk/ felles verdier knyttet til totalsummen og sikringsgruppen havnene og havneanleggene får.

6.1 Kobling mellom konsekvensklasser og klassifisering av havner og havneanlegg

I følge ISPS-kodens del B, 15.5-10 er identifiseringen og vurderingen av viktige verdier og kritisk infrastruktur en prosess som skal ta hensyn til potensialet for tap av liv, havnens økonomiske signifikans, symbolverdi og tilstedeværelse av myndighetsinstallasjoner. Dette blir reflektert i skadevurderingsskjemaet der konsekvensklassene er (i) nedetid/ operativ evne, (ii) miljø, (iii) liv og helse og (iv) omdømme. Ut ifra disse konsekvensklassene har analysegruppen utviklet noen kriterier som sier noe om kritikalitet/viktighet.

"Liv og helse" og "miljø"

ISPS-koden sier at hovedfokuset skal være å "unngå død eller skade". I følge sikkerhetsloven skal man vurdere om det er "mulighet for å utgjøre en fare for miljøet eller befolkningens liv og helse". Derfor benyttes kategorien *antall årlige passasjerer* for å fange opp hvor mange passasjerer som kan rammes. *Antall ansatte* i et havneanlegg er inkludert for å fange opp hvor mange ansatte som til daglig er i havneanlegget. Det var også viktig å se hvordan hendelser i en havn kan påvirke liv og helse til befolkningen som er i nærheten av havnen/havneanlegget. Dermed er kategorien *havneanleggets nærhet til befolkningstette steder* viktig å inkludere når en vurderer kritikalitet. Befolkningstette steder er nærliggende steder der det oppholder seg mye mennesker, f.eks. industri og næringsområder, annen viktig infrastruktur som togstasjoner, eller boligstrøk osv.

[7] (1) Olje og gass, (2) Industri, (3) Cruise, (4) Utenlandsferger, (5) Forsyningsbaser.

Et annet element er farlig gods og farlige stoffer som er i havnen/havneanlegg som kan få konsekvenser for liv og helse, samt miljø. Kategorien *farlig gods og farlige stoffer* skal fange opp dette.

"Operativ evne/ måloppnåelse"

I følge ISPS-koden del B/15.6 er det "viktig å vurdere om havneanlegget, strukturen eller anlegget fortsatt kan fungere uten eiendommen [verdien], og i hvilken grad det er mulig å gjenopprette normal drift raskt". Nedetid for hele virksomheten eller forsinkelser knyttet til viktige leveranser er tett knyttet til økonomi, altså kostnader knyttet til nedetid/forsinkelser av viktige leveranser. Ettersom analysegruppen har et overordnet samfunnsperspektiv var det viktig å tenke hvordan noen havner/havneanlegg har så kritiske leveranser for samfunnet at det vil få store konsekvenser ved nedetid. Dermed ble det laget en egen kategori kalt *strategisk betydning/ redundans*. Dette har blitt sett opp mot nasjonal sikkerhet og suverenitet og kritisk infrastruktur og kritiske samfunnsfunksjoner. Per dags dato finnes det ingen metode/fremgangsmåte for å vurdere om virksomheten er en kritisk samfunnsfunksjon eller faller inn under sikkerhetsloven. Det kreves kvalitative og skjønnsmessige vurderinger. I følge sikkerhetsloven må en vurdere om nedetid kan få betydning for sikkerhetspolitisk krisehåndtering og forsvar av riket, samt kritiske funksjoner for det sivile samfunn. FFI og NKSB har utarbeidet noen tilleggsspørsmål som skal gjøre vurderingen litt lettere. Har havneanlegget (i) import og eksportvarer av strategisk betydning?, (ii) er det bare ditt havneanlegg som utfører spesialiserte operasjoner eller har spesielle verktøy og fasiliteter (f.eks. en type kabler som bare produseres/leveres fra en gitt havn eller utstyr for forsyningssikkerhet)?, (iii) har havneanlegget strategisk betydning for Forsvaret og nærhet til forsvarsinstallasjoner (f.eks. kritisk havneutstyr som RoRo og LoLo)? (iv) er havneanlegget en tidligere «nasjonalt utpekt havn»?.

Kriterier knyttet til havnen/havneanleggets kritikalitet

Fra et overordnet samfunnsperspektiv er det viktig å fange opp havner som er større og mer trafikkerte enn andre. Kategoriene *antall operasjoner i havneanlegg* og *forventet årlig anløp av skip* fanger opp denne dimensjonen. Tanken er også å fange opp kompleksiteten av aktører, operasjoner osv. som skjer i havnen. Vi har også inkludert *terminaltype* med kategorier knyttet til ulik type bulk. [8] Kategoriene ble utarbeidet sammen med KYV og inkluderer en rangering av ulike typer gods: (i) tørrbulk, en-terminals-anlegg for tømmer, stein, grus, asfalt, skrapjern etc., (ii) større gods- og bulkanlegg og stykkgods, (iii) containere og LPG, (iv) forsyningsbaser, olje- og gass-produksjon og cruise, (v) RO/PAX utenlands som er ferge-terminaler for utenlandsferger. Begrunnelsen for denne vektingen er basert på graderte trusselvurderinger og hva som anses som mest målattraktivt for en trusselaktør.

[8] Bulk er "uemballert gods, som stort sett transporteres i store volumer". Våtbulk "er typisk råolje, gass, petroleumsprodukter og kjemikalier, men kan også være matvarer (matolje og juice)". Tørrbulk er definert som "kull, korn, tømmer, malm, metaller, kunstgjødsel og andre typer granulater" (Samferdselsdepartementet 2015:22).

6.2 Kriterier for å beskrive kritikalitet

Analysegruppen vurderte flere kriterier for å vurdere havnen/havneanleggets kritikalitet. Etter møtet med KYV ble det utviklet en modell for å vurdere kritikalitet. Rangeringstabellene tilknyttet hvert kriterie retter seg først og fremst mot kvantitative opplysninger. Flere av terskelverdiene i rangeringstabellene er basert på dansk *best practice* og tilpasset til norske forhold basert på innspill fra KYV. KYV har testet modellen på havneanlegg de har god kjennskap til og deretter kommet innspill til terskelverdiene.

Imidlertid er det for hver av rangeringstabellene et felt hvor vurderingene skal beskrives. Dette er for å ta høyde for de kvalitative vurderingene for hver av kategoriene, og dermed få en mer helhetlig oversikt over de ulike havnene og havneanleggene. Når en legger de ulike rangeringene sammen ender man opp med en poengsum som viser hvilken type sikringsprofil havnen har.

KYV presiserte også to spesifikke krav knyttet til klassifiseringen. Hvis et havneanlegg har over 200 000 årlige passasjerer (altså skår 5, rød farge), vil havneanlegget automatisk havne i sikringsgruppe 3 "svært risikoutsatt". Det andre kravet er knyttet til kriterie "terminaltype". Hvis havneanlegget har RO/PAX (skår 5, rød farge), vil havneanlegget automatisk havne i sikringsgruppe 3 "svært risikoutsatt".

Kategorier	**Beskrivelse**
Antall operasjoner i havneanlegg	Antall operasjoner, flere folk som er knyttet til de ulike fasilitetene osv.
Havneanleggets nærhet til befolkningstette steder	Nærhet til befolkning eller befolkningstette steder (tettbebyggelse, næringsområder, baser, installasjoner med symbolsk verdi og annen infrastruktur).
Antall årlige passasjerer	Forventet tall. Dersom havneanlegget ikke håndterer passasjerer er poengskåren 1 (grønn). Her bør det også vurderes om dette er sesongbasert.
Antall personell som er daglig på havneanlegget	Forventet tall.
Forventet årlig anløp av skip	Forventet tall.
Terminaltype	For eksempel; Håndterer terminalen våtbulk, tørrbulk, containere, stykkgods, passasjer, gass, bygg, RO/PAX utenlands og vedlikehold. Hvis havneanlegget håndterer forskjellige typer gods så tar man utgangspunkt i den godstypen som gir høyest skår.

Farlig gods og farlige stoffer	Begrepet "farlige stoffer" brukes om ethvert stoff som kan utgjøre en urimelig risiko for helse og sikkerhet for operatører, personell eller miljøet hvis det ikke håndteres og behandles korrekt ved lagring, produksjon, foredling, pakking, bruk, destruering eller transport. Når man ser på farene som kan være potensielt skadelige for mennesker bruker man ofte HazMat "diamanten" som er basert på FN's GHS (Globally Harmonized System of Classification and Labelling of Chemicals) og ADR (European Agreement concerning the International Carriage of Dangerous Goods by Road). De farlige stoffene blir gradert etter konsekvensene stoffet har på liv og helse. Vår gradering baserer seg på GHS-diamantens "risikogradering" fra 0-4. For mer informasjon om hvordan dette gjøres, se vedlegg A.
Strategisk betydning/ redundans	Her vurderes det om havneanlegget har strategisk betydning for nasjonal sikkerhet og suverenitet (eksempelvis territoriell suverenitet og integritet, nasjonal handlefrihet, forhold til andre stater, demokratisk styresett eller myndighetenes styringsevne). Det må også vurderes om havneanlegget er en del av kritisk infrastruktur eller kritiske samfunnsfunksjoner (eksempelvis vitale nasjonale interesser som forsyning av energi, mat, vann, samferdsel, telekommunikasjon, helseberedskap, bank- og pengevesen). Det er viktig å tenke på havneanleggets betydning i markedet, og eventuelt om det har nasjonal symbolsk betydning. For å vurdere om havneanlegget har strategisk betydning har FFI og NKSB utarbeidet flere hjelpespørsmål som er i skjemaet (se vedlegg A).

Tabell 6.1 FFI og NKSBs forslag til kriterier for å beskrive havneanleggets kritikalitet.

6.3 Klassifisering av havneanlegg

Formålet med metoden for klassifisering er å identifisere ulike sikringsnivåer for de forskjellige havnene og havneanleggene i Norge. Tidligere benyttet KYV seg av tre grupperinger (i) Grupper 1 – minst risikoutsatt, (ii) Gruppe 2 – Medium, og (iii) Gruppe 3 – Høy. Vi har innenfor denne metoden også vurdert det som hensiktsmessig å operere med tre grupperinger for sikringsnivå: (i) Gruppe 1 – minst risikoutsatt, (ii) Gruppe 2 – mer utsatt, (iii) og (iv) Gruppe 3 – svært utsatt. Begrepene *minst*, *mer* og *svært* kan framstå som tvetydige og det er viktig at KYV definerer hva som ligger i disse begrepene, og hva det vil si å havne innenfor de ulike gruppene. Som nevnt tidligere har KYV har testet modellen på havneanlegg de har god kjennskap til og deretter kommet innspill til terskelverdiene (se tabell 6.2 over havneanleggets sikringsprofil).

Havneanleggets sikringsprofil	
Sikringsgrupper	**Poeng**
Sikringsgruppe 1 – Minst utsatt	**7-16**
Sikringsgruppe 2- Mer utsatt	**17-24**
Sikringsgruppe 3- Svært utsatt	**25-40**

Tabell 6.2 Poengsum knyttet til de ulike sikringsgruppene som har blitt testet av KYV.

Metoden for klassifisering baserer seg både på kvantitative og kvalitative vurderinger. Den kvantitative informasjonen bør være relativt enkelt å samle inn for de ulike havnene og havneanleggene via deres gjennomførte sårbarhetsanalyser, samt deres kunnskap om anleggene og lokalsamfunnet. Det er den kvantitative vurderingen som vil lede til totalsummen og som sier noe om kritikaliteten til havnene. I tillegg er det vurdert som nødvendig å gjennomføre kvalitative vurderinger. Det er trolig mest hensiktsmessig at dette blir gjennomført av KYV. De kvalitative vurderingene kan både øke og senke den totale summen fra de kvantitative vurderingene. De er ment som et supplement der hvor for eksempel objektive tall ikke får fram kompleksiteten eller enkeltheten i systemet. Risikovurderinger for sikringshendelser lar seg vanskelig håndteres med en ren kvantitativ tilnærming, så det vurderes som nødvendig at disse suppleres med skjønnsmessige vurderinger. Under hver av rangeringstabellene er det et felt hvor vurderingene skal beskrives. Her vil det være nyttig å fylle inn informasjon som kan utdype eller forklare de kvantitative vurderingene, og som videre kan gi KYV ytterligere informasjon for å ta en informert beslutning angående endelig sikringsgruppe.

Sikringsgruppene de ulike havnene og havneanleggene ender opp i er ment til å gjøre prosessen for sikring under forhøyet trussel mer effektiv. Likevel er man avhengig av å ha kontinuerlig oppdatert informasjon om trusselnivået og type trussel. Det er ikke å forvente at KYV eller havnene selv skal inneha denne informasjonen, men de må holde seg oppdatert på de åpne trusselvurderingene publisert av PST og E-tjenesten.

7 Anbefalinger til risikobaserte tilsyn og fastsettelse av det maritime sikringsnivået

7.1 Risikobaserte tilsyn og regulering

Ifølge Fimreite, Lango, Lægreid og Rykkja (2014:27) er regulering er nært tilknyttet risiko. De argumenterer for at (i) risiko legitimerer og definerer grunnlaget for regulering og (ii) reguleringsvirksomheten blir organisert, både i form av struktur og prosedyrer, av de risikoer som er nærliggende å ta hensyn til. Regulering er et tvetydig begrep som kan forstås i en vid og en mer begrenset forstand. Fimreite et al. (2014:26) bruker den begrensede definisjonen av regulering, som tar utgangspunkt i en aktivitet som omhandler: "a) formulering av mål, lovgivning, regelutforming, og standardsetting, b) overvåking, inspeksjon, informasjonsinnhenting, tilsyn, revisjon, evaluering og c) håndheving, atferdsmodifisering og bruk av sanksjoner og belønninger".

Lindøe, Kringen og Braut (2015) refererer til et paradigmeskifte innenfor risikobaserte kontrollregimer. I Norge har vi gått fra en regulering basert på lover og forskrifter som ga detaljerte regler for hva som var rett og galt, hvor arbeidsulykker, alvorlige hendelser og farlige arbeidsforhold ble møtt med stadig nye regler. På 1970-tallet fikk et nytt kontrollregime et gjennombrudd, oppmerksomheten ble flyttet fra myndighetenes detaljerte regler til virksomhetens egen kontroll med sikkerheten. Dette innebar at virksomhetene fikk et større ansvar for å vurdere hvilke risikoer som var relevante for dem. I tillegg ble lover og regler endret slik at de la vekt på å beskrive hvilke mål virksomhetene skulle nå i sitt sikkerhetsarbeid, og hvordan de skulle nå disse målene (Lindøe, Kringen og Braut 2015). I korte trekk kan paradigmeskiftet forklares med at det gikk fra *command-and-controll-tilnærming* til en reguleringstilnærming som i større grad fokuserte på frihet, selvstendighet og beslutningsmyndighet på lavere nivå.

Tilsyn kan, ifølge Fimreite et al. (2014) betraktes som den utøvende delen av regulering. "Regulering fungerer som et grunnlag for tilsynet og forteller hva som skal oppnås, og hvilke hensyn som skal beskyttes, samt hva det skal føres tilsyn med og hvilke krav som er satt" (Fimreite et al. 2014:105). Med utgangspunkt i Stortingsmelding 17 (2002-2003:22-23) forklarer Lindøe, Kringen og Braut (2015) at tilsynsbegrepet, i vid forstand, kan forstås som et fellesbegrep for all aktivitet eller bruk av virkemidler som iverksettes for å følge opp et lovverks intensjoner. Kjernen i tilsynsrollen er imidlertid den konkrete kontrollen av pliktobjektets etterlevelse av en norm, som allerede er fastsatt ved lov, forskrift eller enkeltvedtak, samt reaksjoner ved eventuelle avvik. I tillegg til tilsyn som kontroll og reaksjoner på avvik skal tilsynet gi tilsynsobjektene generell informasjon om reguleringens formål, om regelverkets krav og lignende temaer som har betydning for dem regelverket retter seg mot. Et slikt informasjonsarbeid følger av forvaltningslovens veiledningsplikt. En sentral del av tilsynsrollen blir dermed å oppsøke eller på annet vis å innhente informasjon om tilsynsobjekter for å avdekke og følge opp eventuelle avvik fra myndighetskrav (Lindøe, Kringen og Braut 2015).

Lindøe et al. (2015:124) definerer risikobasert tilsyn som "en utpeking av virksomheter og sikkerhetsrelevante forhold for tilsyn på grunnlag av en vurdering av hvor og når helsemessige, sikkerhetsmessige eller miljømessige forhold er høyest". Risikobasert tilsyn blir dermed et grunnlag for prioritering av tilsynsinnsatsen, og dreier seg om å prioritere tilsynsressursene slik at de rettes mot virksomheter med størst risiko (Lindøe, Kringen og Braut 2015). I så måte kan man si at risikobasert tilsyn tar høyde for at prioriteringer ikke bare kan ta utgangspunkt i et regelverk. I følge Baldwin, Cave og Lodge (2012) er det noen sentrale elementer som går igjen i de forskjellige rammeverkene for risikobasert tilsyn. For det første krever risikobasert tilsyn at den som fører tilsyn identifiserer sine egne målsetninger, og risikoen tilsynsobjektene utgjør for evnen til å nå disse målene. For det andre må tilsynsorganet lage et system hvor risikoene vurderes og gis verdi (risikoscore). Hvordan man tilnærmer seg risikovekting/score varierer betydelig. Noen systemer har en kvalitativ tilnærming mens andre er kvantitativt orientert. De ulike risikoene rangeres vanligvis av virksomheten etter brede kategorier som høy, medium og lav, eller mer findelte inndelinger uttrykt i tall eller flere kategorier (Baldwin, Cave og Lodge 2012).

Når det gjelder risikobasert tilsyn skiller Baldwin og Black (2010) mellom iboende risiko og risiko tilknyttet virksomhetens ledelse og risikostyring. De iboende risikoene er risiko forbundet med produksjonsprosessen og området/omgivelsene omkring sine iboende egenskaper. Dette kan for eksempel være bruk av giftige substanser som kan skade nærliggende økosystemer eller naturressurser man ønsker å skjerme. Dette kan også være relatert til prosesser hvor små feilmarginer kan ha store konsekvenser. Risikofaktorer som er knyttet til styring og ledelse handler om virksomhetens evne til å håndtere de iboende risikoene på en god måte gjennom ledelse og internkontroll (Baldwin og Black 2010). Dette vil videre si at både iboende risiko og evnen til å håndtere disse må vurderes. Dette betyr at en virksomhet som i utgangspunktet har mye iboende risiko i praksis kan være sikker om virksomheten har implementert tilstrekkelig med sikkerhetstiltak og tatt høyde for dette i sine beredskapsplaner.

7.2 Utfordringer med risikobasert tilsyn

For tilsynsmyndigheter handler det om å finne balansen mellom (i) å sikre at tilsynspersonellet har godt funderte vurderinger og (ii) sikre at vurderingene blir relativt like, uavhengig av hvem som gjør dem. Risikovurderinger krever at tilsynsmyndighet gjør vurderinger basert på skjønn. Det er en sentral utfordring for tilsynsmyndigheter å styre hvordan skjønn utøves og gjøre vurderinger av risiko konsistente, uten å gjøre tilsynsregimet dyrt, rigid og lite responsivt (Baldwin, Cave og Lodge 2012).

Baldwin, Cave og Lodge (2012) trekker fram flere utfordringer ved implementering av risikobasert tilsyn. En utfordring er å avgjøre i hvilken grad risikobasert tilsyn skal drive regulators handlinger. Problemet som kan oppstå er at noen risikoevalueringer har større nytteverdi i forhold til noen typer reguleringsoppgaver enn andre. Dette kan lede fokus mot høyrisikoområder, aktører og aktiviteter, men gi lite veiledning til hvilke virkemidler som er best egnet for å redusere risikoen.

Det kan være utfordrende å få den risikobaserte tilsynstilnærmingen til å fungere i en organisasjon. Som en del av risikobasert tilsyn må den regulerende myndighet ta enkelte egne vurderinger tilknyttet forhold som for eksempel ledelses- og styringsrisiko. Det kan være krevende for regulator å sikre at disse egenvurderingene er konsistente, uten at man gjør tilsynsregimet kostbart og for rigid (Baldwin, Cave og Lodge 2012). En mulig forutsetning for å kunne lykkes med implementeringen av risikobasert tilsyn er å skape kulturelle endringer i tilsynsorganet for å bevege praksisen vekk fra de eldre og mer regelfokuserte tilsynsregimene. Om ikke denne endringen skjer risikerer man at man tilpasser det nye systemet slik at det produserer de samme resultatene som det gamle systemet.

En annen sentral utfordring med risikobasert tilsyn, og risikohåndtering generelt, er at regimet må håndtere potensielle uoverensstemmelser i forbindelse med regulators og offentlighetens risikopersepsjon. Dette kan kompliseres ytterligere ved at risikopersepsjon ikke er statisk, og preferanser for hvordan man skal utføre regulering endres ofte. Typisk vil en alvorlig hendelse kunne påvirke offentlighetens krav og aksept for regulering og tilsyn. Eksempelvis foretrakk mange land minst mulig inngripende regulering av finansnæringen før finanskrisen, mens det i etterkant har oppstått betydelig politisk press fra velgere, media, regjering og tilsynsmyndigheter for å føre en mer aktiv og aggressiv regulering av sektoren. På samme måte har terrorhendelser her hjemme og nærliggende land skapt en økt aksept og etterspørsel fra enkelte for sikkerhetsreguleringer, etterretning og overvåking. Baldwin, Cave og Lodge (2012) peker på at det kan være vanskelig å tilpasse seg til nye endringer når en tilsynsmyndighet har besluttet å følge et gitt rammeverk. Dette gjør seg særlig gjeldende når prosessen med å skape og utvikle rammeverket er begravd dypt i byråkratiske prosesser, og dermed skjermet mot presset fra offentligheten og media.

En ytterligere utfordring kan oppstå når tilsynsmyndigheten skal prioritere mellom forebygging av små, men hyppige ulykker, og store, men sjeldne ulykker. Storulykker får ofte mer oppmerksomhet og kan fort utvikle seg til å bli en politisk betent sak. Dette leder videre til at tilsynsmyndighet i større grad blir eksponert for politisk press i kjølvannet av storulykker, og har dermed et insentiv for å prioritere denne typen ulykker til tross for at flere skader og dødsfall forårsakes av små og hyppige ulykker. I så måte kan man si at regulator handler i tråd med demokratiske impulser, men det kan diskuteres hvorvidt en slik tilnærming i praksis vil være formålstjenlig for å beskytte samfunnet (Baldwin, Cave og Lodge 2012).

Rettferdiggjøring av beslutninger gjort på bakgrunn av risikobasert tilsyn kan også være mer utfordrende enn metodikken tilsier. Inkludert i ideen om risikobasert tilsyn ligger den forlokkende tanken om at kompleksiteten og utfordringene med regulering kan rasjonaliseres, ledes og kontrolleres. Gjennom risikoidentifikasjon, evaluering og validering skyves usikkerhet og uforutsigbarhet unna, og leder til en rasjonell, åpen og kostnadseffektiv regulerings- og tilsynsprosess (Baldwin, Cave og Lodge 2012). I praksis betyr dette at toppledelsen må tydeliggjøre hvor langt de er villige til å gå i bruken av risikobasert regulering. Hvis de ikke gjør dette vil det kunne lede til at den utførende delen av organisasjonen fatter tiltak for å skjerme seg mot kritikk ved å vektlegge andre faktorer enn risikoanalysen. Dette vil videre kunne bidra

til å redusere rasjonaliteten i tilsynsregimet (Lindøe, Kringen og Braut 2015 og Baldwin, Cave og Lodge 2012).

7.3 Regulering av og tilsyn med security-relaterte risikoer

Jore og Moen (2015) referer til to ulike regimer i forbindelse med regulering av risiko; det risikobaserte regimet og det regelbaserte regimet. I artikkelen blir de ulike regimene sett opp mot security-relatere risikoer. Forfatterne hevder at de to regimene ikke er gjensidig utelukkende, men heller komplementære. Diskusjonen vil dermed ikke være hva som er best, men hvordan man på best mulig måte kan balansere disse to. Jore og Moen (2015) poengterer at det er fordeler og ulemper med begge regimene. Det regelbaserte, ovenfra og ned command-and-control-regimet, vil på den ene siden sørge for at alle virksomheter som arbeider med, for eksempel, havneanlegg forholder seg til de samme reglene. Dette gjør at virksomheten i mindre grad må ta beslutninger og prioritere mellom sikringstiltak, men heller fokusere på å følge reglene. På den andre siden vil et for stort fokus på reglene kunne medføre at det ikke rettes oppmerksomhet mot å holde virksomheten så sikker som mulig, da det stilles få krav til innovative sikringsløsninger og tilpasninger til nye risikoer. En sentral utfordring med et regelbasert regime, og kanskje særlig innenfor sikringsfeltet, er at det kan være vanskelig å tilpasse til et raskt skiftende trusselbilde (Jore og Moen 2015). Å endre lover og regler er en tidkrevende prosess og kan i verste fall føre til at trusselen blir reell før den nødvendige reguleringen er på plass. Ofte kan man se at store ulykker eller alvorlige hendelser kan skape store endringer i sikkerhetsreguleringer, hvor det beste eksemplet kanskje er den store forandringen i flyplassikkerheten etter 11. september 2001.

Risikobasert regulering bygger på antakelsen om at organisasjoner relatert til, - eller eiere av, kritisk infrastruktur innehar den nødvendige kompetansen for å vurdere hvilke risikoer de kan møte i framtiden samt at de vet hvordan de kan håndtere disse. Dette innebærer at risikovurderinger bør være en del av beslutningsstøtten i beslutningsprosessen for å sikre at de riktige valgene blir tatt med tanke på å finne det optimale nivået av sikkerhet (Jore og Moen 2015). Risikobasert regulering kan sees i sammenheng med den såkalte trefaktortilnærmingen, introdusert gjennom to nye norske standarder utgitt i 2012 og 2014 (NS 5830:2012 og NS 5832:2014). Dette betyr at virksomhetene vurderer hvilke trusler som er relevante for dem, identifiserer verdier og sårbarheter og implementerer tilstrekkelige sikringstiltak. Den største fordelen med risikobasert regulering, forutsatt at virksomheten er kjent med sine verdier, sårbarheter og relevante trusler, er at de kan prioritere sikringstiltakene der hvor de er mest sårbare. Tilnærmingen kan også sies å være mer fleksibel og mer kompatibel med et skiftende trusselbilde, da virksomhetene selv kan endre sikringsinnretningen om nye trusler skulle bli aktuelle.

Som nevnt i kapittel 5.7 er security-relaterte risikoer tilknyttet stor grad av usikkerhet som både vil ha påvirkning på risikovurderingen og de tiltak som iverksettes som følge av vurderingen. For tilsiktede uønskede handlinger, og særlig terrorhandlinger, vil trusselaktøren som utgjør risikoen være en kalkulerende og tilpasningsdyktig person. Dette betyr at trusselaktøren kan tilpasse seg implementerte sikringstiltak og endre sin modus operandi. De som vurderer risikoen

må være klar over dette. Med dette som bakgrunn kan en risikobasert regulering være hensiktsmessig for security-relaterte risikoer da denne tilnærmingen "tvinger" virksomhetene å benytte risikovurderingene aktivt og kontinuerlig holde seg oppdatert på aktuelle trusler. Dette anses som en mer hensiktsmessig måte å tilpasse sikkerhetstilstanden på enn å følge en sjekkliste over regler, som en regelbasert tilnærming maner til. En risikobasert regulering vil imidlertid kreve bredere kompetanse hos virksomheten da den fordrer at virksomheten selv skal ha oversikt over risikoene som er relevante for dem. Det er langt fra alle virksomheter som har denne kompetansen tilgjengelig, og må kanskje støtte sine beslutninger på nasjonale eller kjøpte risikovurderinger (Jore og Moen 2015).

Delkapitlet ble introdusert med at diskusjonen ikke bør dreie seg om hva som er best tilnærming til regulering, men hvordan man på best mulig måte kan balansere risikobasert og regelbasert regulering. Det er jo ikke slik at det ene utelukker det andre. Selv om risikobasert regulering velges som den rådende tilnærming vil det fortsatt være lover og regler som styrer deler av arbeidet. Regelbasert regulering vil lede til en uniform implementering av sikringstiltak, hvor myndighetene setter krav, og alle virksomheter innenfor en bransje vil ha samme sikringsnivå (Jore og Moen 2015). En slik tilnærming er for eksempel rådende innenfor flybransjen. Risikobasert regulering vil kreve at virksomheten har kunnskap om deres verdier, sårbarheter og relevante trusler, og ut ifra dette implementere tiltak hvor det anses som nødvendig. Utfordringen knyttet til security-relaterte risikoer er at disse hendelsene er lavfrekvente og tilknyttet stor usikkerhet (Jore og Moen 2015). Risikobasert regulering vil dermed framstå som mer fleksibel, men vil kreve mer sikringskompetanse innad i virksomheten.

7.4 Tilsynsrollen

På samme måte som risikobasert regulering kan være mer krevende enn regelbasert regulering for virksomheten, vil også tilsynsrollen være annerledes. Innenfor et regelbasert regime vil tilsyn kunne sies å være enklere, da det i all hovedsak vil innebære å kontrollere at virksomheten følger de gjeldende reglene. Mens det innenfor et risikobasert regime vil være nødvendig å forholde seg til ulike tilsynskrav hos ulike aktører, og større krav til å sørge for at det er gjennomført risikovurderinger og implementert tiltak (Jore og Moen 2015). Tilsynsrollen har dermed gått fra å være kontrollerende til mer veiledende.

7.5 Anbefalinger knyttet til risikobaserte tilsyn

FFI og NKSBs anbefalinger til risikobaserte tilsyn er forsøkt tilpasset Kystverkets virkeområde. I tillegg er de basert på de ovennevnte teoretiske bidragene og erfaringer fra FFI.[9]

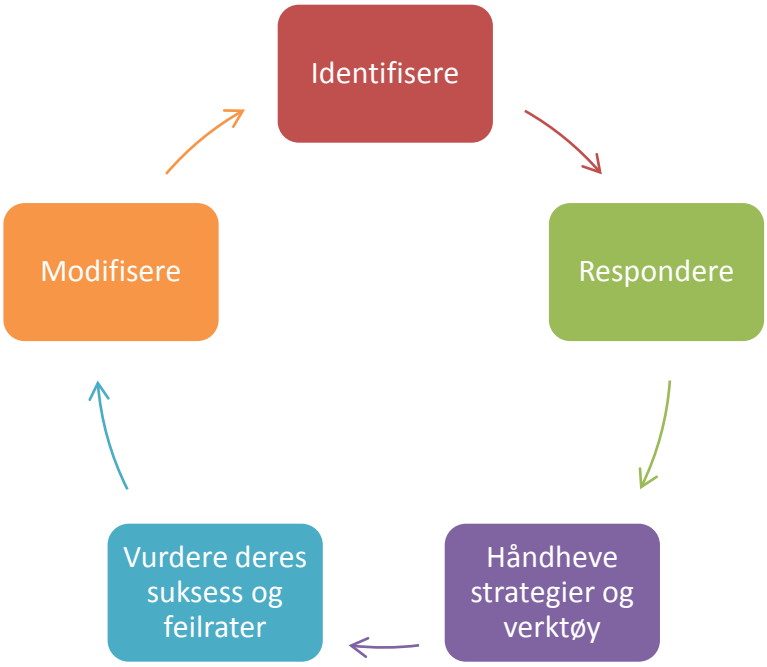
En av Kystverkets oppgaver er å føre tilsyn med norske havner og havneanlegg. Disse er av forskjellig størrelser, har ulike og mer eller mindre kritiske funksjoner, har ulik kapasitet og

[9] Intervju med Marit Bjerknes (FFI) 5. oktober 2016 på FFI, Kjeller. Bjerknes har bred tilsynserfaring fra Arbeidstilsynet, Næringslivets sikkerhetsorganisasjon (NSO) og FFI

ligger spredt over hele Norge. Dette betyr videre at enkelte havner potensielt vil kunne være mer sårbar i forbindelse med security-relaterte risikoer enn andre. Under den forhøyede uspesifiserte terrortrusselen mot Norge sommeren 2014 måtte Kystverket, som mange andre virksomheter, øke sikringsnivået på ved alle sine havner. De manglet en klassifisering av havnene, og alle havnene måtte derfor anses som like kritiske.

Det som er felles for alle havner og havneanlegg, og som er viktig for grunnlaget for tilsyn, er at man er avhengig av at samspillet mellom menneske, teknologi og organisasjon (MTO) skal fungere. Dette samspillet vil være like viktig å kartlegge i alle havner og havneanlegg. For å unngå at tilsyn bare er gjennomgang av en sjekkliste må det også tas hensyn til hvorvidt og hvordan de ulike punktene er blitt implementert hos aktørene. Blir beredskapsplanene øvet? Kjenner de ulike medarbeiderne sine roller ved en potensiell ulykke? Er tilstrekkelig opplæring gitt til personell som er ansvarlig for de ulike teknologiene og systemene? For at samspillet mellom MTO skal fungere er man avhengig av at (i) menneskene har tilstrekkelig opplæring, (ii) teknologien er tilpasset og forstått for de oppgavene som skal gjennomføres og at (iii) organisasjonen har tilstrekkelig systemer for å fange opp eventuelle mangler eller avvik.

Figur 7.1 introduserer en modell for risikobasert tilsyn som basert på retningslinjene for "really responsive risk" (Black og Baldvin 2010:183). De ulike trinnene i modellen går ut på å (i) identifisere, (ii) respondere, (iii) håndheve strategier og verktøy, (iv) vurdere deres suksess og feilrater og (v) modifisere.



Figur 7.1 Risikobasert tilsyn (basert på retningslinjene for «really responsive risk») (Black og Baldvin 2010:183).

Identifisere

Startpunktet for modellen ovenfor er identifikasjon av risikoer eller uønsket atferd. Her vil det være viktig å kartlegge relevante risikoer hos de ulike havnene og havneanleggene. Metoden for klassifisering, som er gjennomgått i vedlegg A, i tillegg til gjennomførte risikovurderinger (PFSA'ene) anbefales som et utgangspunkt her. Videre anbefales det at hver av havnene eller havneanleggene gjennomfører disse vurderingene selv eller, i det minste, er involvert i vurderingsprosessen. Dette er viktig av flere årsaker. For det første er det disse aktørene som har best kjennskap til sin egen organisasjon, både når det gjelder personell og prosesser. I tillegg innehar de den nødvendige lokalkunnskapen for best å kunne vurdere mulige konsekvensene av en sikringshendelse. For det andre vil eierskap til risikovurderingen kunne påvirke videre aksept og engasjement i prosessen, og man unngår at risikovurderingen blir et skjema bortgjemt i en skuff. I denne prosessen vil det også være formålstjenlig å innhente informasjon om tidligere sikringshendelser, nestenulykker og sikringshendelser i nærliggende virksomheter i andre land. Bjerknes (2016) kommenterer også at de har dratt nytte av å motta en "selvangivelse fra virksomhetene". Dette innebærer at de har sendt ut spørreskjemaer hvor de ansatte i virksomhetene selv har fått kartlegge positive og negative sider knyttet til sikring ved sin arbeidsplass. Dette kan være en krevende oppgave, men kan lede til et mer helhetlig situasjonsbilde, som vil være forankret på flere nivåer i virksomhetene.

På et strategisk nivå, i dette tilfellet Kystverket, vil det være mulig å definere ulike risikogrupper. På security-siden vil typiske elementer å basere sikringsgruppene på være frakt av farlig gods, passasjertransport, utenlandsk skipstrafikk og nærhet havnene eller havneanleggene har til by/tettsted m.m. På safety-siden vil ulykker, nestenulykker og andre brudd på regelverket være elementer som kan være med å bestemme hyppigheten på tilsyn.

Respondere

I denne fasen er hovedoppgaven å utvikle verktøy for å håndtere de identifiserte risikoene og den uønskede atferden. Her er det å anbefale at det utformes en generell grunnsikring for de ulike havneanleggene, og basert på kritikaliteten deres mer spesifikke tiltak. Det bør i tillegg, på bakgrunn av klassifiseringen, være forhåndsbestemt hvilke tiltak som skal igangsettes ved en eventuell forhøyet trussel. Historikk over tidligere inntrufne hendelser bør også være med å utforme hensiktsmessig respons hvor tilstrekkelig opplæring, rutiner og nødvendig utstyr bør vektlegges.

Håndheve strategier og verktøy

På bakgrunn av identifikasjon og respons skal de valgte tiltakene og verktøyene håndheves. Her vil for eksempel hyppigheten av tilsyn være relevant. For utpekte sårbare eller kritiske objekter kan det vurderes om det bør gjennomføres hyppigere tilsynsrunder. Dette kan graderes på lignende måte som for klassifiseringsmetoden, og man kan for eksempel velge intervaller som hvert 5. år for de med laveste risikonivå, hvert 3. for de i den midterste gruppen og hvert år for de med høyest risikonivå. FFI (2016) anbefaler også å føre hyppigere tilsyn med de virksomheter som utpeker seg som høyrisikoområder. Dette bør utformes på bakgrunn av de

konsekvenser risikoene kan ha på liv/helse, miljø, materiell, verdier og omdømme. Tilsynshyppigheten bør også innrettes etter hvor det er mulighet, vilje og evne til å gjøre endringer (FFI 2016).

Hvis det innføres nye tiltak og regler er det å gjennomføre øvelser en god måte å sørge for at disse er implementert og forstått av virksomhetene. Det bør derfor inngå i tilsynsrundene å kontrollere at dette er gjennomført og på hvilke måter virksomheten har tilpasset seg endringene.

Vurdere suksess og feilrater

Dette er kanskje modellens mest utfordrende punkt. Det er nesten umulig å vurdere effekten tilsyn har på risikonivået (FFI 2016). Det som likevel vil være nødvendig er å være bevisst på det strategivalget man har tatt. Her er det bestemt hvilke områder det skal fokuseres på og hvilke elementer man har lagt til grunn for disse valgene. Ved tilsyn vil kanskje disse elementene vektlegges og ser man at virksomhetene har fulgt retningslinjene vil det trolig også kunne sammenlignes med hendelsesstatistikker. Innenfor security-området er det, som nevnt, lite forskning på effekt av sikringstiltak. Dette vil også være en utfordring når det gjelder tilsyn. Det vil være vanskelig, om ikke umulig, å undersøke hvorvidt de implementerte sikringstiltakene har hatt effekt eller om trusselen ikke var tilstede.

Modifisere

Dette er et viktig punkt, og det understrekes at modellen for tilsyn ikke er statisk, men dynamisk. Pilene i modellen kunne gått begge veier og på kryss og tvers fra de ulike delene. Som nevnt tidligere kan Kystverket basere tilsynshyppigheten sin på risikokategorier. Det vil heller ikke være hensiktsmessig at disse er statiske, men at risikonivåene tilpasset etter tilsynsrunder.

7.6 Fastsettelse av det maritime sikringsnivået

For fastsettelse av det maritime trusselnivået må de ulike sikringsprofilene fungere veiledende, men hvilket sikringsnivå som blir satt vil avhenge av type trussel/omfang. Det må være en konkret vurdering i hvert enkelt tilfelle. FFI og NKSB anbefaler at klassifiseringsmetoden knyttet til hvert havneanlegg skal bli gjennomført av havneanlegget selv. Når det er flere havneanlegg i en havn vil havneanlegget med høyest poengsum være dimensjonerende og det man tar utgangspunkt i for hele havnen. Når det har skjedd en trusselforhøyelse kan KYV heve sikringsnivået etter den operasjonen som bedrives i det aktuelle tidsrommet.

I klassifiseringsmetoden er det flere kvalitative beskrivelser som KYV må ta hensyn til. KYV bør også ta hensyn til tidligere sikringshendelser i havneanlegget eller havnen. Dette har KYV i et eget hendelsesregister, noen eksempler er bombetrusler, tyveri av gods, hærverk, blindpassasjerer, menneskesmugling, spionasje, terror/sabotasje. Dette må Kystverket vurdere ved en generell trusselforhøyelse.

8 Konklusjon og veien videre

FFI har i samarbeid med NKSB har utarbeidet en metode for klassifisering av norske havneanlegg og kommet med anbefalinger til risikobaserte tilsyn. Rapporten har beskrevet analysegruppens fremgangsmåte og avgrensninger, samt hva slags datamateriale som har blitt lagt til grunn.

Gjennom arbeidsmøter og innspill fra KYV har det blitt utviklet ulike kriterier for å bedømme kritikalitet, med tilhørende rangeringstabeller. Med kritikalitet menes hvor kritisk havnen eller havneanlegget er. Noen eksempler på kriterier knyttet til havneanlegg er antall årlige passasjerer, hva slags type gods som blir lagret og fraktet og havneanleggets strategiske betydning. Åtte rangeringstabeller blir brukt for hvert enkelt havneanlegg for å bestemme hvilken samlet poengsum de får, og dermed hvilken sikringsprofil de tilhører (gruppe 1 – minst risikoutsatt, gruppe 2 – mer utsatt og gruppe 3 – svært utsatt). Deretter må man se havneanleggets poengsum opp mot de andre ISPS-havneanleggene i havnen. Alle havneanlegg i en gitt havn må dimensjoneres etter den høyeste poengsummen.

FFI og NKSB anbefaler at KYV arrangerer kurs eller en lansering av tilnærmingen slik at sektoren (KYV og RSO'ene) får en omforent forståelse av hvordan man klassifiserer havneanlegg. FFI og NKSB anbefaler også at klassifiseringsmetoden er testet på forhånd av KYV slik at de ulike poengsummene kan tilpasses sikringsprofilene.

FFI og NKSB har beskrevet generelle trusseltrender innen maritim sektor. Trusselvurderingen fokuserer på kategoriene terror, etterretning, sabotasje og annen kriminalitet. Analysen har benyttet trendrapporter fra Kripos, Politiets sikkerhetstjeneste, Etterretningstjenesten, forskningsrapporter fra FFI samt internasjonale databaser over terrorhendelser. FFI og NKSB har også hatt samtaler med PST om generelle trusseltrender i Norge. KYVs hovedkontor har presentert sitt hendelsesregister med ulike typer trusler og sikringshendelser i deres sektor. Dette var nyttig som grunnlag for å beskrive trusseltrendene.

Denne studien anbefaler at KYV baserer sine risikobaserte tilsyn på havnenes sikringsprofil, som følge av klassifiseringen, samt havnenes egne gjennomførte sårbarhetsvurderinger. Hyppigheten av tilsyn bør vurderes med hensyn til både hvor kritisk havnen er og erfaringer fra tidligere tilsyn. Grunnlaget for tilsynet bør være bredt forankret, og de ulike havneanleggene selv bør være involvert i prosessen med klassifiseringen og sårbarhetsvurderingene. I rapporten vises det til en modell for risikobasert tilsyn. Modellen og anbefalingene baserer seg på teoretiske bidrag fra relevant faglitteratur og praktiske erfaringer.

Studien har utført noen vurderinger knyttet til dagens system:

- *I denne sektoren gjennomfører man "sårbarhetsvurderinger", men i praksis er dette det man i andre sektorer betegner som en risikovurdering. Det kan derfor være nødvendig å gjøre dette klart i veiledninger og lignende, for å unngå begrepsforvirring.*

- *Burde drifter eller eier anlegget være sin egen RSO? Dette kan føre til at havneanlegget selv har mer eierskap til PFSA'en og drar nytte av prosessen som trengs for å gjennomføre en sårbarhetsvurdering. KYV har også en egen veileder som kan brukes. Ofte er det nødvendigvis ikke resultatene av en PFSA som er det viktigste, men at prosessen rundt utarbeidelsen (Busmundrud et al 2015:67).*

Forkortelser

ADR	European Agreement concerning the International Carriage of Dangerous Goods by Road
FFI	Forsvarets forskningsinstitutt
GHS	Globally Harmonized System of Classification and Labelling of Chemicals
IMO	International Maritime Organization
ISPS	International Ship & Port facility Security code
ISSC	International Ship Security Certificate
KYV	Kystverket
LO-LO	Lift off-lift on
NKSB	Nasjonalt kompetansesenter for sikring av bygg
NSM	Nasjonal sikkerhetsmyndighet
PFSA	Port facility security assessment
PFSO	Port facility security officer
PSO	Port security officer
PFSP	Port facility security plan
PST	Politiets sikkerhetstjeneste
RO-RO	Roll off-roll on
RSO	Recognized security organization
SOLAS	The International Convention for the Safety of Life at Sea
TAPS	Technical aspects and port security

Vedlegg A Metode for klassifisering av norske havner og havneanlegg

Fremgangsmåte for klassifisering av havneanlegg og havner steg-for-steg	
Formålet med denne klassifiseringen av havneanlegg og havner er å identifisere hvilke havner som tilhører ulike sikringsprofiler. Det er 3 sikringsprofiler: Gruppe 1 – Minst risikoutsatt, Gruppe 2 – Mer risikoutsatt, Gruppe 3 – Svært risikoutsatt. Denne klassifiseringen kan bli brukt hvis det skjer en generell heving av trusselnivået for å bestemme hvilke havner som må opp på et høyere sikringsnivå.	
Steg 1	Les tabell 1 og bli kjent med de ulike kategoriene som blir brukt for å sette poeng. Fyll ut tabellen med en beskrivelse, se gjerne vedlagt eksempel. Det er mulig å trekke mye informasjon ut ifra havneanleggets PFSA.
Steg 2	Et havneanlegg får poeng basert på de parameterne som er skissert i tabell 1. Bruk rangeringstabellene og inkluder en kvalitativ beskrivelse på hvert punkt.
Steg 3	Fyll inn poengsummen i tabell 2 og regn ut totalsummen for rangeringstabellene.
Steg 4	Se hva slags sikringsprofil havneanlegget har basert på poengsummen. Deretter må man se havneanleggets poengsum opp mot de andre ISPS-havneanlegget i havnen. Alle havneanlegg i en gitt havn må dimensjoneres etter den høyeste poengsummen. Eksempel: Ved en forhøyet uspesifisert trussel må ISPS-havneanlegg 1 med lav poengsum som ligger i nærhet til ISPS-havneanlegg 2 med høy poengsum forholde seg til beredskapsnivået som anses nødvendig for ISPS-havneanlegg 2. Tabell 3 som viser havnens sikringsprofil vil være gjeldende ved en forhøyet trussel. Her er det også en egen boks med en kvalitativ beskrivelse av vurderingen.

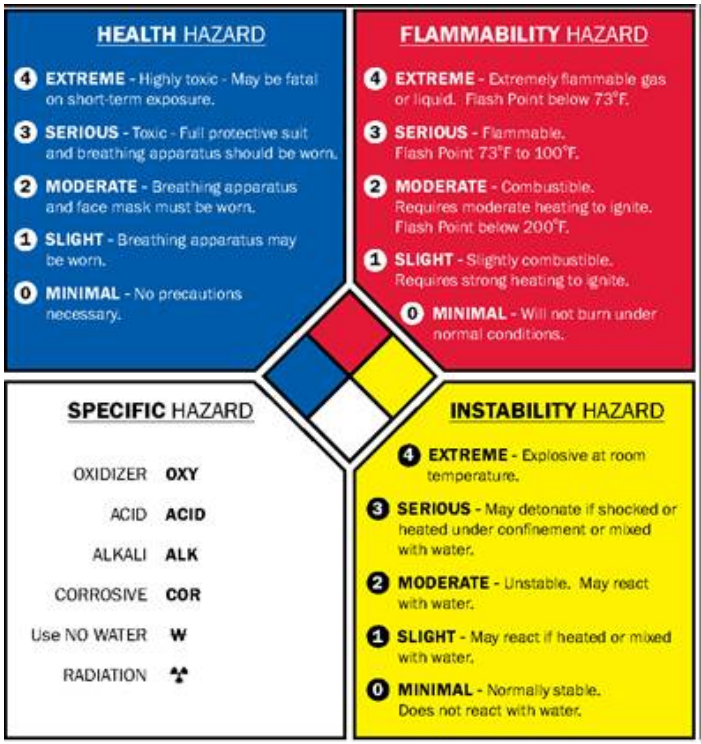
Tabell 1	
Kategorier	**Beskrivelse**
Antall operasjoner i havneanlegg	Antall operasjoner, flere folk som er knyttet til de ulike fasilitetene osv.
Havneanleggets nærhet til befolkningstette steder	Nærhet til befolkning eller befolkningstette steder (tettbebyggelse, næringsområder, baser, installasjoner med symbolsk verdi og infrastruktur).
Antall årlige passasjerer	Forventet tall. Dersom havneanlegget ikke håndterer passasjerer er risikoskåren 1 (grønn). Her bør det også vurderes om dette er sesongbasert.
Antall personell som er daglig på havneanlegget	Forventet tall.
Forventet årlig anløp av skip	Forventet tall.
Terminaltype	For eksempel; Håndterer terminalen våtbulk, tørrbulk, containere, stykkgods, passasjer, gass, bygg, RO/PAX utenlands og vedlikehold. Hvis havneanlegget håndterer forskjellige typer gods så tar man utgangspunkt i den godstypen som gir høyest skår.
Farlig gods og farlige stoffer	Begrepet "farlige stoffer[10]" brukes om ethvert stoff som kan utgjøre en urimelig risiko for helse og sikkerhet for operatør- eller beredskapspersonell, offentlig eller miljøet hvis ikke det håndteres og behandles korrekt ved lagring, produksjon, foredling, pakking, bruk, destruering eller transport.

[10] Definisjonen av Farlig stoff er « (i) Brannfarlig stoff: Fast, flytende eller gassformig stoff, stoffblanding, samt stoff som forekommer i kombinasjoner av slike tilstander, som i kraft av sitt flammepunkt, kontakt med andre stoffer, trykk, temperatur eller andre kjemiske egenskaper representerer en fare for brann. (ii) Reaksjonsfarlig stoff: Fast, flytende, eller gassformig stoff, stoffblanding, samt stoff som forekommer i kombinasjoner av slike tilstander, som ved kontakt med vann, ved sitt trykk, temperatur eller andre kjemiske forhold, representerer en fare for farlig reaksjon, eksplosjon eller utslipp av farlig gass, damp, støv eller tåke. (iii) Trykksatt stoff: Annet fast, flytende eller gassformig stoff eller stoffblanding enn brann- eller reaksjonsfarlig stoff, som er under trykk, og som derved kan representere en fare ved ukontrollert utslipp. Definisjonen av farlig stoff er en innsnevring i forhold til brann- og eksplosjonsvernlovens definisjon i § 4 c) da denne også omfatter eksplosjonsfarlig stoff». (*Forskrift om håndtering av brannfarlig, reaksjonsfarlig og trykksatt stoff samt utstyr og anlegg som benyttes ved håndteringen*).

Når man ser på farene som kan være potensielt skadelige for mennesker bruker man ofte HazMat "diamanten" som er basert på FN's GHS (Globally Harmonized System of Classification and Labelling of Chemicals) og ADR (European Agreement concerning the International Carriage of Dangerous Goods by Road).

De farlige stoffene blir gradert etter konsekvensene stoffet har på liv og helse. I fotnotene er det eksempler på hva slags type farlige stoffer dette kan være kategorisert etter de (i) helseskadelige farene (blå), (ii) brannfaren (rød), (iii) sensitivitet/stabilitet (gul) og (iv) andre spesifikke farlige kjemiske egenskaper som oksyderende, radioaktiv, reaktiv med vann etc. (hvit). Grunnen til at man deler det opp på denne måten er fordi et kjemikalie kan godt ha flere av disse egenskapene på en gang. En giftig forbindelse kan f.eks. også være brennbar.

Vår gradering baserer seg på GHS-diamantens "risikogradering" fra 0-4. De giftige forbindelsene (blå) vil være *direkte* skadelige på helse og liv da de avhenger av eksponering, mens de brennbare og ustabile (rød og gul) vil være mere *indirekte* da man jo er avhengig at det er mennesker tilstede hvis en brann eller eksplosjon forekommer.



Strategisk betydning/ redundans	Her vurderes det om havneanlegget har strategisk betydning for nasjonal sikkerhet og suverenitet (eksempelvis territoriell suverenitet og integritet, nasjonal handlefrihet, forhold til andre stater, demokratisk styresett eller myndighetenes styringsevne). Det må også vurderes om havneanlegget er en del av kritisk infrastruktur eller kritiske samfunnsfunksjoner (eksempelvis vitale nasjonale interesser som forsyning av energi, mat, vann, samferdsel, telekommunikasjon, helseberedskap, bank- og pengevesen). Det er viktig å tenke på havneanleggets betydning i markedet, og eventuelt om det har nasjonal symbolsk betydning. For å vurdere om havneanlegget har strategisk betydning kan dette være nyttige hjelpespørsmål: (i) Har havneanlegget import og eksportvarer av strategisk betydning?, (ii) Er det bare ditt havneanlegg som utfører spesialiserte operasjoner eller har spesielle verktøy og fasiliteter (f.eks. en type kabler som bare produseres/leveres fra en gitt havn eller utstyr for forsyningssikkerhet)? (iii) Har havneanlegget strategisk betydning for Forsvaret og nærhet til forsvarsinstallasjoner (f.eks. kritisk havneutstyr som RoRo og LoLo)?, (iv) Tilhører havneanlegget en tidligere «nasjonalt utpekt havn»?.

Rangeringstabell 1: Antall operasjoner

Antall	1	2	3	4	+5
Poeng	1	2	3	4	5
Beskriv vurderingene					

Rangeringstabell 2: Havneanleggets nærhet til befolkningstette steder

Antall	Over 3 km distanse fra befolkningstette steder	2-3 km distanse fra befolkningstette steder	1-2 km distanse fra befolkningstette steder	300m-1 km distanse fra befolkningstette steder	Mellom 0-300 m til befolkningstette steder
Poeng	1	2	3	4	5
Beskriv vurderingene					

Rangeringstabell 3: Antall årlige passasjerer					
Antall	<1000	1001- 50.000	50 001-100.000	100 001 -200.000	Over 200.001
Poeng	1	2	3	4	5
Beskriv vurderingene					

Rangeringstabell 4: Antall personell i havneanlegget					
Antall	0-5	6-20	21-50	51-200	Over 200
Poeng	1	2	3	4	5
Beskriv vurderingene					

Rangeringstabell 5: Forventet årlig anløp av skip					
Antall	<50	51-150	151-300	301-500	Over 500
Poeng	1	2	3	4	5
Beskriv vurderingene					

Rangeringstabell 6: Terminaltype					
Antall	Tørrbulk En-terminals-anlegg for tømmer, stein, grus, asfalt, skrapjern etc.	Større gods- og bulkanlegg og stykkgods.	Containere og LPG.	Forsyningsbaser. Olje- og gass-produksjon. Cruise	(RO/PAX utenlands) Ferge-terminaler for utenlands-ferge.
Poeng	1	2	3	4	5
Beskriv vurderingene					

Rangeringstabell 7: Farlig gods og farlige stoffer			
	Har havneanlegget farlige stoffer som har konsekvenser under 2 (minimal eller liten fare, se HazMat "diamanten").	Havneanlegg som oppbevarer farlige stoffer til eget bruk og som ofte er lokalisert med viss distanse til kaiområdet. Dette gjelder farlige stoffer med konsekvenser over 2: moderat, seriøs og ekstrem fare (se HazMat "diamanten").	Har havneanlegget farlige stoffer som har konsekvenser over 2 (moderat, seriøs og ekstrem fare, se HazMat "diamanten").
Poeng	0	3	5
Beskriv vurderingene			

Rangeringstabell 8: Strategisk betydning/ redundans			
	Havneanlegget har ikke noen påvirkning på nasjonal sikkerhet og suverenitet (eksempelvis territoriell suverenitet og integritet, nasjonal handlefrihet, forhold til andre stater, demokratisk styresett eller myndighetenes styringsevne). Havneanlegget kan heller ikke sies å være en del av kritisk infrastruktur eller kritiske samfunnsfunksjoner (eksempelvis vitale nasjonale interesser som forsyning av energi, mat, vann, samferdsel, telekommunikasjon, helseberedskap, bank- og pengevesen).	Har havneanlegget: • Import og eksportvarer av strategisk betydning? • Er det bare ditt havneanlegg som utfører spesialiserte operasjoner eller har spesielle verktøy og fasiliteter (f.eks. en type kabler som bare produseres/leveres fra en gitt havn eller utstyr for forsyningssikkerhet)?	Har havneanlegget: • Har havneanlegget strategisk betydning for Forsvaret og nærhet til forsvarsinstallasjoner (f.eks. kritisk havneutstyr som RoRo og LoLo)? • Tilhører havneanlegget en tidligere «nasjonalt utpekt havn»?
Poeng	0	3	5
Beskriv vurderingene			

Tabell 2: Oppsummering av ditt havneanlegg									
	Antall operasjoner	**Havneanleggets nærhet til belfolkningstette steder**	**Antall årlige passasjerer**	**Antall personell i havneanlegget**	**Forventet årlig anløp av skip**	**Terminal-type**	**Farlig gods og farlige stoffer**	**Strategisk betydning/ redundans**	**Poengsum**
Poeng									

Havneanleggets sikringsprofil	
Sikringsgrupper	**Poeng**
Sikringsgruppe 1 – Minst utsatt	**7-16**
Sikringsgruppe 2- Mer utsatt	**17-24**
Sikringsgruppe 3- Svært utsatt	**25-40**

Tabell 3: Havnens sikringsprofil[11]		
Gruppe 1 – Minst risikoutsatt	**Gruppe 2 – Mer risikoutsatt**	**Gruppe 3 – Svært risikoutsatt**
[Havner med alle havneanlegg under poeng 7-16]	**[Havner med havneanlegg mellom poengsummen 17-24]**	**[Havner med havneanlegg mellom poengsummen 25-40]**
Beskriv vurderingene:		

[11] I tilfeller der det er flere ISPS-havneanlegg i én havn vil havneanlegget med høyest poengsum angi klassifiseringsnivået for havnen i en situasjon med forhøyet trusselnivå, jf. hendelsene sommeren 2014. Eksempel: Ved en forhøyet uspesifisert trussel må ISPS-havneanlegg 1 med lav poengsum som ligger i nærhet til ISPS-havneanlegg 2 med høy poengsum forholde seg til beredskapsnivået som anses nødvendig for ISPS-havneanlegg 2. Alle havneanlegg i en gitt havn må dermed dimensjoneres etter den høyeste poengsummen.

Metode for klassifisering av havneanlegg: Eksempel

Hjertvik havneanlegg- Midt Norge
Havneanlegget som vurderes Midthavna, Hjertvik havneanlegg. *Eieren* er Midthavna AS. *Operatører:* Flere bedrifter har drift på havneanlegget. Felles for alle er at Hjertvik A/S er en direkte som agent/eller som innleid operatør forstår den sikringsrelaterte driften av skip-land operasjon (ISPS).

Tabell 1	
Kategorier	**Beskrivelse**
Antall operasjoner i havneanlegget	Det er flere operasjoner på havneanlegget: Deriblant lagringsplass for ulik type bulk, tankanlegg, kontorlokaler og verksted/lager for eksplosiv service (dette bygget ligger atskilt fra hovedhallen med murvegger).
Havneanleggets nærhet til befolkningstette steder	-Havneanlegget ligger i nærheten av fylkesveien. -Småbåthavn 250 meter fra havneanlegget -Ingen bebyggelse eller strandsone med bolig eller fritidshus i nærheten. -Halsøy gassanlegg ligger i umiddelbar nærhet. De lagrer og tar i mot propangass.
Antall årlige passasjerer	Havneanlegget håndterer ikke passasjerer.
Antall personell som er daglig på havneanlegget	Det er maksimum 50 personer som er på havneanlegget daglig.

Forventet årlig anløp av skip	Mellom 50-100 anløp av skip årlig.
Terminaltype	Hjertvik havneanlegg håndterer: -tørrbulk (salt), -våtbulk (LPG), -det har vært en begrenset mengde med stykkgods og prosjektlaster.
Farlige gods og farlige stoffer	Det er noen kystgodsskip som frakter gods til Nord-Norge, bl.a. sprengstoff som blir fraktet til gruveindustri i Nord-Norge. Eksplosivene kommer til havneanlegget med lastebil fra Oslo og har et tidsbegrenset transittopphold i havneanleggets bygg før frakt på kystgodsskip.
Strategisk betydning/ redundans	Per dags dato er har ikke Hjertvik havneanlegg import og eksportvarer av strategisk betydning. Det har blitt diskutert om havneanlegget skal være en lossehavn for flydrivstoff til luftforsvaret, men det er ikke noen planer om å bygge et anlegg for dette i nærmeste fremtid. Hvis dette blir aktuelt kan havneanlegget få strategisk betydning for Forsvaret og en ny vurdering trengs

Rangeringstabell 1: Antall operasjoner					
Antall	1	2	3	4	+5
Poeng	1	2	3	✓ 4	5
Beskriv vurderingene	*Eksempel: Lagringsplass for ulik type bulk, tankanlegg, kontorvirksomhet og verksted/lager for eksplosiv service (dette bygget ligger atskilt fra hovedhallen med murvegger).*				

Rangeringstabell 2: Havneanleggets nærhet til befolkningstette steder					
Antall	Over 3 km distanse fra befolkningstette steder	2-3 km distanse fra befolkningstette steder	1-2 km distanse fra befolkningstette steder	300m-1 km distanse fra befolkningstette steder	Mellom 0-300 m til befolkningstette steder
Poeng	✓ 1	2	3	4	5
Beskriv vurderingene	*Eksempel: Havneanlegget er ikke i nærheten av symbolsk beliggenhet (historisk/kulturelt) der det kan være et stort antall personer. Det er ikke noe nærliggende kritisk infrastruktur og dermed ikke et stort antall av personer.*				

Rangeringstabell 3: Antall årlige passasjerer					
Antall	<1000	1001- 50.000	50 001-100.000	100 001 -200.000	Over 200.001
Poeng	✓ 1	2	3	4	5
Beskriv vurderingene	*Eksempel: Ettersom det ikke er passasjertrafikk, men godstrafikk blir ikke havneanlegget påvirket av sesongene.*				

Rangeringstabell 4: Antall personell i havneanlegget					
Antall	0-5	6-20	21-50	51-200	Over 200
Poeng	1	2	✓ 3	4	5
Beskriv vurderingene	*Eksempel: Det er maksimum 50 personer som er på havneanlegget daglig.*				

Rangeringstabell 5: Forventet årlig anløp av skip					
Antall	<50	51-150	151-300	301-500	<500
Poeng	1	✓ 2	3	4	5
Beskriv vurderingene	*Eksempel: Mellom 50-100 anløp av skip årlig.Skip som skal til England fra liten kai attraktivt for blindpassasjer.*				

Rangeringstabell 6: Terminaltype					
Antall	Tørrbulk En-terminals-anlegg for tømmer, stein, grus, asfalt, skrapjern etc.	Større gods- og bulkanlegg og stykkgods.	Containere og LPG.	Forsyningsbaser. Olje- og gass-produksjon. Cruise	(RO/PAX utenlands) Ferge-terminaler for utenlands-ferge.
Poeng	1	2	✓ 3	4	5
Beskriv vurderingene	*Eksempel: tørrbulk (salt), våtbulk (LPG), det har vært en begrenset mengde med stykkgods og prosjektlaster.*				

Rangeringstabell 7: Farlig gods og farlige stoffer			
	Har havneanlegget farlige stoffer som har konsekvenser under 2 (minimal eller liten fare, se HazMat "diamanten").	Havneanlegg som oppbevarer farlige stoffer til eget bruk og som ofte er lokalisert med viss distanse til kaiområdet. Dette gjelder farlige stoffer med konsekvenser over 2: moderat, seriøs og ekstrem fare (se HazMat "diamanten").	Har havneanlegget farlige stoffer som har konsekvenser over 2 (moderat, seriøs og ekstrem fare, se HazMat "diamanten").
Poeng	0	3	✓ 5
Beskriv vurderingene	*Eksempel: Dette havneanlegget har flere typer av farlige gods; LPG og eksplosiver/dynamitt. Det er noen kystgodsskip, bl.a. frakter sprengstoff til gruveindustrien i Nord-Norge. Eksplosivene kommer til havneanlegget med lastebil fra Oslo og har et tidsbegrenset transittopphold i havneanleggets bygg før frakt på kystgodsskip. Et annet forhold er Vestli gassanlegg med propangass som ligger rett ved.*		

Rangeringstabell 8: Strategisk betydning/redundans			
	Havneanlegget har ikke noen påvirkning på nasjonal sikkerhet og suverenitet (eksempelvis territoriell suverenitet og integritet, nasjonal handlefrihet, forhold til andre stater, demokratisk styresett eller myndighetenes styringsevne). Havneanlegget kan heller ikke sies å være en del av kritisk infrastruktur eller kritiske samfunnsfunksjoner (eksempelvis vitale nasjonale interesser som forsyning av energi, mat, vann, samferdsel, telekommunikasjon, helseberedskap, bank- og pengevesen).	Har havneanlegget: • Import og eksportvarer av strategisk betydning? • Er det bare ditt havneanlegg som utfører spesialiserte operasjoner eller har spesielle verktøy og fasiliteter (f.eks. en type kabler som bare produseres/leveres fra en gitt havn eller utstyr for forsyningssikkerhet)?	Har havneanlegget: • Har havneanlegget strategisk betydning for Forsvaret og nærhet til forsvarsinstallasjoner (f.eks. kritisk havneutstyr som RoRo og LoLo)? • Tilhører havneanlegget en tidligere «nasjonalt utpekt havn»?
Poeng	✓ 0	3	5
Beskriv vurderingene	*Eksempel: Hvis Luftforsvaret har lyst til å bruke havneanlegget til å losse flydrivstoff kan det bli mer målattraktivt. Per dags dato er har ikke Hjertvik havneanlegg import og eksportvarer av strategisk betydning. Det har blitt diskutert om havneanlegget skal være en lossehavn for flydrivstoff til luftforsvaret, men det er ikke noen planer om å bygge et anlegg for dette i nærmeste fremtid. Hvis dette blir aktuelt kan havneanlegget få strategisk betydning for Forsvaret og en ny vurdering er nødvendig.*		

Tabell 2: Oppsummering av ditt havneanlegg									
	Antall operasjoner	**Havne-anleggets nærhet til befolknings-tette steder**	**Antall årlige passasjerer**	**Antall personell i havne-anlegget**	**Forventet årlig anløp av skip**	**Terminal-type**	**Farlig gods og farlige stoffer**	**Strategisk betydning/ redundans**	**Poeng-sum**
Poeng	4	1	1	3	2	3	5	0	**19**

Havneanleggets sikringsprofil	
Sikringsgrupper	**Poeng**
Sikringsgruppe 1 – Minst utsatt	**7-16**
Sikringsgruppe 2- Mer utsatt	**17-24**
Sikringsgruppe 3- Svært utsatt	**25-40**

Tabell 3: Havnens sikringsprofil		
Gruppe 1 – Minst risikoutsatt	**Gruppe 2 – Mer risikoutsatt**	**Gruppe 3 – Svært risikoutsatt**
[Havner med alle havneanlegg under poeng 7-16]	**Hjertvik havneanlegg fikk poengsummen 19. [Havner med havneanlegg mellom poengsummen 17-24].**	**[Havner med havneanlegg mellom poengsummen 25-40]**

Referanser

Asal, V. og Justin V. Hastings, J. V (2014). *Terror at Sea: Exploring Maritime Targeting by Terrorist Organizations*. Sist besøkt 10.06. 2016. http://piracy-studies.org/terror-at-sea-exploring-maritime-targeting-by-terrorist-organizations/

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

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

Bakir, N. O. (2007). *A Brief Analysis of Threats and Vulnerabilities in the Maritime Domain*. Non-published Research Reports. Paper 5. Sist besøkt 10.06. 2016. http://research.create.usc.edu/nonpublished_reports/5

Baldwin, R. og Black, J. (2010). "Really responsive risk based regulation" in *Law and policy*, s. 181-213.

Baldwin, R., Cave, M. og Lodge, M. (2012). *Understanding regulation: Theory, Strategy, and Practice* (2.utg.). New York: Oxford University press.

Busmundrud, O., Maal, M., Hagness Kiran, J. og Endregard, M (2015). *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger*. FFI-rapport 2015/00923. https://www.ffi.no/no/Rapporter/15-00923.pdf

Center for the Protection of Critical Infrastructure (2013*). CPNI Insider Data Collection Study: report of main findings*. Publisert april 2013.

Center for the Protection of Critical Infrastructure (2013). *Personnel Security Risk Assessment*.

DSB (2014). Nasjonalt risikobilde 2014. Sist besøkt 30. november 2016. http://www.dsb.no/Global/Publikasjoner/2014/Tema/NRB_2014.pdf

Eggereide, B. Kråkenes, T. Fridheim, H. (2007). *Innenriks sjøfart som mål for terror - en risikovurdering*. FFI/RAPPORT-2007/00004 (Begrenset).

Elgsaas, I. M. og Heireng, H. S (2014). *Norges sikkerhetstilstand – en årsaksanalyse av mangelfull forebyggende sikkerhet*. FFI-rapport 2014/00948.

EU (2004). "Regulation (EC) No 725/2004", *regulation by the European Parliament and of the Council of*

March 2004 on enhancing ship and port facility security, datert 31.03.04.

EU (2005). "Directive 2005/65/EC", *Directive of the European Parliament and of the Council on 26 October 2005 in enhancing port security, datert 26.10.05.*

EU (2008). "Commission Regulation (EC) No 324/2008 of 9 April 2008", *revised procedures for conducting Commission inspections in the field of maritime security, datert 09.04.08.*

Europol (2016). Changes in modus operandi of Islamic State terrorist attacks. Sist besøkt 11.11. 2016. https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-terrorist-attacks

Fimreite, A.L., Lango, P., Lægreid, P. og Rykkja, L.H. (2011). *Organisering, samfunnssikkerhet og krisehåndtering.* Oslo: Universitetsforlaget.

Fischhoff, B. (2002). *Assessing and Communicating the Risks of Terrorism*. Sist besøkt 27.10.2016. http://www.orau.gov/cdcynergy/erc/content/activeinformation/resources/FischhoffAAAS.pdf

Fiskeri- og kystdepartementet (2004). *Forskrift om sikkerhet og terrorberedskap i norske havner*. 23. juli 2004 nr. 1017

Forsvarsbygg (2016). *Sikringshåndboka*. Andre utgave. Ventes utgitt desember 2016.

Forsvarsdepartementet, *Lov om forebyggende sikkerhetstjeneste* (Sikkerhetsloven) av 20. mars 1998 nr. 10 med endringer, sist ved lov av 11. april 2008 nr. 9 (i kraft 1. januar 2011

Fridheim, H., Tor-Erik Schjelderup, T., og Borander, A. (2009). *Viljeshandlinger mot kollektivtransport i storbyer – trusler og tiltak*. FFI-rapport 2009/01078

Global Teorrism Database (2015a). *Incident summary Achille Lauro*. Sist besøkt 10.06. 2016. https://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=198510070028

Global Teorrism Database (2015b). *Incident summary USS Cole*. Sist besøkt 10.06. 2016. https://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=200010120001

Global Terrorism Database (2015c). *Incident summary MV Limburg*. Sist besøkt 10.06. 2016. https://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=200210060001

International Maritime Organization (2003). *ISPS Code*. 2003 Edition

International Maritime Organization (2012). *Guide to Maritime Security and the ISPS Code*, 2012 Edition, IMO Publication, London.

Jore, S. H. og Moen, A. (2015). A discussion of the risk-management and the rule-compliance regulation

regimes in a security context. *Safety and reliability: Methodology and Application.*

Jore, S. H. og Njå, O., (2010). *Risk of Terrorism: A Scientifically Valid Phenomenon or a Wild Guess? The Impact of Different Approaches to Risk Assessment.* Universitetet i Stavanger.

Kripos (2014). *Den organiserte kriminaliteten i Norge – trender og utfordringer 2015.* Oktober 2014.

Kystverket (2011). "Losloven" på Kystverkets nettsider, publisert 2011. Sist besøkt 22. september 2016. http://www.kystverket.no/Regelverk/Losloven/

Kystverket (2011). *Veiledning om havne- og farvannsloven*. Publisert 29. september 2011, tilgjengelig elektronisk på Kystverkets nettsider, sist besøkt 21. september 2016.10.27 http://www.kystverket.no/Regelverk/Havne--og-farvannsloven/

Kystverket (2016a). *Hva er kystverket?* Sist besøkt 28.04.2016. http://www.kystverket.no/Om-Kystverket/Kva-er-Kystverket/

Kystverket (2016b). *Kystverkets organisering*. Sist besøkt 10.06. 2016. http://www.kystverket.no/Om-Kystverket/Kva-er-Kystverket/Organisering/

Kystverket (2016c). *Kystverkets mål og visjon.* Sist besøkt 28.04.2016. http://www.kystverket.no/Om-Kystverket/Kva-er-Kystverket/Mal-og-visjon/

Kystverket (2016d). *Kystverket sitt virke*. Sist besøkt 10.06. 2016. http://www.kystverket.no/Om-Kystverket/Kva-er-Kystverket/Verksemd/

Lindøe, P., Kringen, J. og Braut, G. S. (2015) *Risiko og tilsyn: Risikostyring og rettslig regulering* (2.utg.). Oslo: Universitetsforlaget.

Lovdata (2008). *Lov om forebyggende sikkerhetstjeneste (*Sikkerhetsloven) av 20.03.98, med endringer, sist vedtatt ved lov av 11.04.08.

Lovdata (2013). *Forskrift om sikring av havneanlegg*. FOR-2013-05-29-538

Nesser, P., og Stenersen, A. (2014a). "The modus operandi of jihadi terrorists in Europe" I *Perspectives on terrorism*. Volume 8 issue 6. ISSN 2334-3745.

Nesser, P., og Stenersen, A. (2014b). *The modus operandi of jihadi terrorists in Europe*. Foredrag under FFI-forum den 28.10.2014

Nesser, P., Stenersen, A. og Oftedal, E. (2016). *Jihadi Terrorism in Europe: the IS-effect*. Draft paper fra seminaret "European Jihadism in the 'Caliphate' Era" holdt i Oslo 1- 2. september 2016.

Nincic, D. (2012). "Maritime Terrorism: How Real is the Threat?" i *Fair observer*. Sist besøkt 10.06.

2016. http://www.fairobserver.com/region/north_america/maritime-terrorism-how-real-threat/

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

NS (2014a). *Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikostyring.* Norsk Standard NS 5831:2014.

NS (2014b). *Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til*

sikringsrisikoanalyse. Norsk Standard NS 5832:2014.

NSM (2016). *Håndbok for risikovurdering for sikring*. Nasjonal sikkerhetsmyndighet, mars 2016.

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

PST (2013). *Periodisk gjennomgang av obligatorisk sårbarhetsvurdering for innenriks sjøtransport og av havneanlegg som betjener slik trafikk*. Begrenset.

PST (2016). *Trusselvurdering 2016*. Sist besøkt 01.10. 2016.
http://www.pst.no/media/81096/PST_Brosjyre_Trussel_NORSK.pdf

RAND (2006). *Maritime Terrorism - Risk and Liability*. Sist besøkt 10.06. 2016.
http://www.rand.org/content/dam/rand/pubs/monographs/2006/RAND_MG520.pdf

Regjeringen (2015). *Nasjonal havnestrategi 2015*. Sist besøkt 10.06. 2016.
https://www.regjeringen.no/contentassets/7a2d341125bc485ebdb0065e5ad1db05/nasjonal_havnestrategi_21012015.pdf

Rutledal, Frode (2002a). *Systembeskrivelse av norsk sjøtransport*. FFI/RAPPORT-2002/01363.

Rutledal, Frode (2002b). *Vurdering av sårbarheten i norsk sjøtransport.* FFI-RAPPORT-2002/04551 (Konfidensielt).

Sikkerhetslovutvalget (2016). *Samhandling for sikkerhet*. NOU 2016: 19. Sist besøkt 10.11.2016
https://www.regjeringen.no/no/dokumenter/nou-2016-19/id2515424/sec1

About FFI

The Norwegian Defence Research Establishment (FFI) was founded 11th of April 1946. It is organised as an administrative agency subordinate to the Ministry of Defence.

FFI's MISSION

FFI is the prime institution responsible for defence related research in Norway. Its principal mission is to carry out research and development to meet the requirements of the Armed Forces. FFI has the role of chief adviser to the political and military leadership. In particular, the institute shall focus on aspects of the development in science and technology that can influence our security policy or defence planning.

FFI's VISION

FFI turns knowledge and ideas into an efficient defence.

FFI's CHARACTERISTICS

Creative, daring, broad-minded and responsible.

Om FFI

Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs FORMÅL

Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

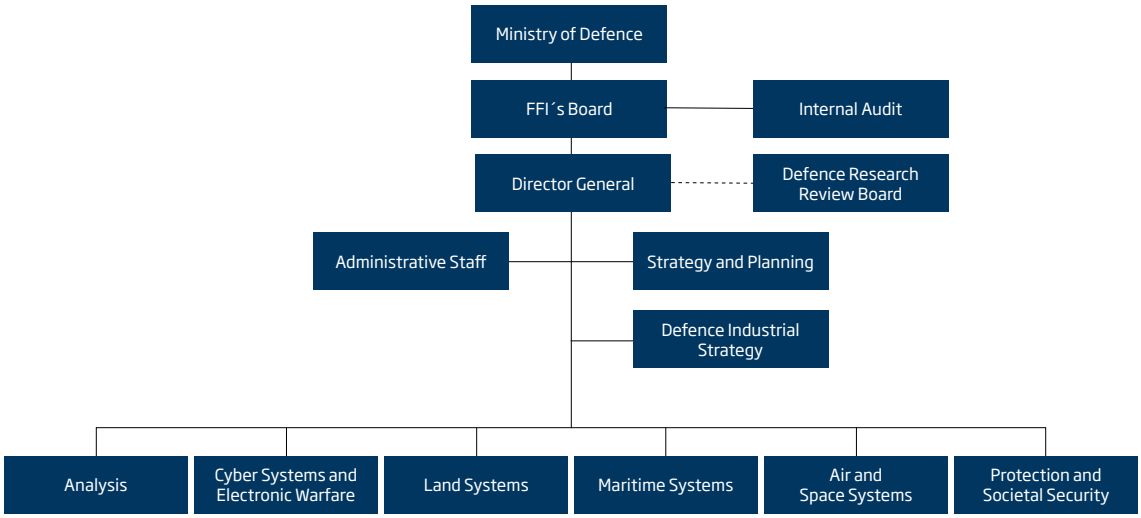
FFIs VISJON

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs VERDIER

Skapende, drivende, vidsynt og ansvarlig.

FFI's organisation



Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

Telefon: 63 80 70 00
Telefaks: 63 80 71 15
Epost: ffi@ffi.no

Norwegian Defence Research Establishment (FFI)
P.O. Box 25
NO-2027 Kjeller

Office address:
Instituttveien 20
N-2007 Kjeller

Telephone: +47 63 80 70 00
Telefax: +47 63 80 71 15
Email: ffi@ffi.no

FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment