Høgskulen på Vestlandet

Bacheloroppgave

NAB3030-PRO-1-2023-VÅR-FLOWassign

Predefinert informasjon

Startdato:	19-04-2023 00:00 CEST	**Termin:**	2023 VÅR
Sluttdato:	03-05-2023 14:00 CEST	**Vurderingsform:**	Norsk 6-trinns skala (A-F + Bestått)
Eksamensform:	Bacheloroppgave		
Flowkode:	203 NAB3030 1 PRO-1 2023 VÅR		
Intern sensor:	(Anonymisert)		

Deltaker

Navn:	Johan Wichmann
Kandidatnr.:	228
HVL-id:	593379@hvl.no

Informasjon fra deltaker

Antall ord *:	13959

Egenerklæring *:	Ja
Jeg bekrefter at jeg har registrert oppgavetittelen på norsk og engelsk i StudentWeb og vet at denne vil stå på vitnemålet mitt *:	Ja

Gruppe

Gruppenavn:	DVH
Gruppenummer:	8
Andre medlemmer i gruppen:	Øyvind Wang, Fredrik Bjerkenes Hanssen

Jeg godkjenner avtalen om publisering av bacheloroppgaven min *

Ja

Er bacheloroppgaven skrevet som del av et større forskningsprosjekt ved HVL? *

Nei

Er bacheloroppgaven skrevet ved bedrift/virksomhet i næringsliv eller offentlig sektor? *

Nei

Høgskulen på Vestlandet

BACHELOROPPGAVE

Hva ligger i skipssikkerhetsforskriftens krav om at det må gjøres en sårbarhetsvurdering for skip?

What is the requirement in the Ship Safety and Security Regulations that a vulnerability assessment must be made for ships?

219 Fredrik Bjerkenes Hanssen

225 Øyvind Wang

228 Johan Wichmann

Bachelor Nautikk

Fakultet for økonomi og samfunnsvitenskap

Institutt for maritime studium

Veileder: Professor Sigmund Simonsen

03.05.2023

Jeg bekrefter at arbeidet er selvstendig utarbeidet, og at referanser/kildehenvisninger til alle kilder som er brukt i arbeidet er oppgitt, *jf. Forskrift om studium og eksamen ved Høgskulen på Vestlandet, § 12-1.*

FORORD

Denne bacheloroppgaven markerer avslutning for oss som 3 studenter på Nautikk ved HVL i Haugesund. Nautikkstudiet har vært krevende, med tanke på oppstart under korona-pandemien og en studiehverdag preget av mye hjemmeundervisning. Vi har jobbet godt gjennom tre raske og krevende år, og vi ser frem til å endelig bli uteksaminerte alle tre.

Vi har diskutert masse, og drøftet på hva det er vi har lyst til å vie vår bacheloroppgave til. Vi ble etter hvert veldig interessert i temaet "maritime security" og valgte videre å se på sårbarhetsvurdering, noe som var et felt hvor det var gjort lite forskning med tanke på norske farvann. Dette er da noe vi har lyst til å fremheve og kartlegge da vi mener dette er et tema som fortjener mer fokus.

Vi vil rette en stor takk til vår veileder, professor Sigmund Simonsen som har hjulpet oss og veiledet oss til rett vei for å ferdigstille oppgaven vår. Vi vil også takke representant fra Sjøfartsdirektoratet som tok seg tid til å snakke med oss om vår bacheloroppgave.

Haugesund, 3 mai 2023

---------- ----------

Fredrik B. Hanssen *Johan Wichmann*

Øyvind Wang

SAMMENDRAG

I en verden som stadig er i utvikling og hvor nye utfordringer skapes, er det mange momenter det skal tas hensyn til med tanke på sikkerhet. Sikkerhetssituasjonen i Nord-Europa er i endring i lys av krigen i Ukraina, noe som også er aktuelt for norske farvann og norske skip. Etter mange år med fred og få bekymringer, er sikkerheten i våre egne farvann i endring. Sabotasje mot Nord Stream-gassledningene i Østersjøen, ukjente brudd på undervannskabler og større etterretningsaktivitet i norsk sektor er blant momentene som vekker bekymring.

For å løse denne oppgaven har vi brukt juridisk metode hvor drøfting har vært et stort fokus. Dette er fordi det er lite rettskilder å henvise til i ISPS- koden. Vi har også bladd opp i forskrifter og forordninger rundt temaet ISPS for å ta for oss kravene rundt sårbarhetsvurdering. ISPS koden ble dannet i 2002 med grunnlag for å begrense terrorhandlinger og øke maritim sikkerhet. Den kom senere inn i norsk forskrift i 2004. Videre så retter vi fokus mot rettspraksisen rundt sårbarhetsvurdering hvor vi ser på relevansen rundt de bindende punktene i ISPS koden.

Sikkerhetsforskriften dekker et stort omfang med å inkorporere ISPS koden inn i lovverket. Dette bidrar til en omfattende sårbarhetsvurdering om utarbeidingen er gjort grundig. Vi ser likevel at ISPS-koden kanskje burde vært bedre, der datasikkerhet kunne fått sitt eget punkt. Dette nevnes på grunn av utviklingen av cyberteknologi og sårbarheten for at cyberangrep er blitt mye større og relevant. Utover utviklingen av teknologi, så er det også kommet mye mer informasjon og data som må beskyttes. Derfor mener vi fokuset rundt cyber og ISPS må bli bedre.

Nå etter nyere handlinger gjennom krigen mellom Ukraina og Russland, har også Norge blitt en av de større gassleverandørene til Europa, så er det på tide at sårbarhetsvurderingene oppdateres.

ABSTRACT

In a world that is constantly evolving and where new challenges are being created, there are many factors that must be taken into account with regard to security. The security situation in Northern Europe is changing in light of the war in Ukraine, which is also relevant for Norwegian waters. After many years of peace and few concerns, security in our own waters is changing. Sabotage against the Nord Stream gas pipelines in the Baltic Sea, unknown ruptures of subsea cables and major intelligence activity in the Norwegian sector are among the factors that give rise to concern.

To solve this assignment, we have used legal methodology where discussion has been a major focus. This is because there are few legal sources to refer to in the ISPS code. We have also browsed through regulations and regulations around the topic of ISPS to address the requirements around vulnerability assessment. The ISPS Code was formed in 2002 with the basis for limiting terrorist acts and increasing maritime security. It was later incorporated into Norwegian regulations in 2004. Furthermore, we focus on the case law on vulnerability assessment, where we look at the relevance of the binding points in the ISPS Code.

The security regulations cover a large scope of incorporating the ISPS code into legislation. This contributes to a comprehensive vulnerability assessment if the preparation has been done thoroughly. However, we see that perhaps the ISPS code should have been better, where data security could have gotten its own point. This is mentioned because of the development of cyber technology and the vulnerability to cyber attacks becoming much larger and relevant. In addition to the development of technology, there is also much more information and data that needs to be protected. Therefore, we believe the focus around cyber and ISPS must be improved.

Now, after recent actions through the Ukraine-Russia war, Norway has also become one of the larger gas suppliers to Europe, it's time for vulnerability assessments to be updated.

INNHOLDSFORTEGNELSE

1.0 INNLEDNING

1.1 TEMA

Fokuset omkring maritim sikkerhet så en stor økning etter 9/11. Tidligere hadde man ikke tenkt på skip som særlige terrormål, men hendelsen i USA førte til bevissthet rundt dette. Skip, grunnet deres store størrelse og potensielle energi, ble vurdert til å kunne utgjøre mål og brukes til terror. Etter 9/11, var IMO (International Maritime Organization) raskt ute med et regelverk som fikk forkortelsen ISPS (International Ship and Port Facility Security.) Det nye regelverket kom med krav til sikkerhetstiltak for skip og havner over hele verden. Piratvirksomhet har alltid vært et problem for den internasjonale skipsfarten. Pirater søker ikke nødvendigvis å forårsake skade, men heller økonomisk vinning, et av formålene med ISPS-koden er derfor også å forhindre ran og kapring av skip.

Nå i nyere tid med mye politisk uro i verden, hvor Russlands krig mot Ukraina preger den sikkerhetspolitiske situasjonen i verden, så er kanskje regelverket utdatert? Sikkerhetssituasjonen påvirker naturlig også det maritime segmentet, der vi ser Nord-Stream ledningene bli sabotert, droner flyes nært kritisk infrastruktur og en generell økning i hendelser tilknyttet sikkerhet i Nord-Europa.
Politiets sikkerhetstjeneste, Nasjonale sikkerhetsmyndigheter og Etterretningstjenesten belyser også den sikkerhetspolitiske situasjonen i dag ved sine respektive trusselvurderinger. Der de viser til en generell trend hvor de ser en klar opptrapping av etterretningsvirksomhet fra nasjonale aktører, spesielt nasjoner som Russland.

Per dags dato (Mars 2023) så er det lite sannsynlig at Russland vil drive med sabotasje i Norge, men sabotasje kan bli en realitet fra Russland ved en eventuell eskalering. (PST, 2023, s.4.) Dette gjenspeiles blant annet i at Norge har valgt å heve sikkerhetsnivået på mange av sine havner, noe som fører til at skip må øke sikkerhetsnivået sitt. Som tidligere nevnt er det stor etterretningsaktivitet fra Russland, hvor man ser en økning i bruken av sammensatte trusler. Sammensatte trusler er en form for bruk av flere metoder og hendelser der den kombinerte sammensetningen brukes for å oppnå en ønsket målsetting. *"Sammensatte trusler kan forekomme i sikkerhetspolitiske gråsoner, der formålet er å skape splid og destabilisering."* (Nasjonal Sikkerhetsmyndighet, 2023, s.12)

Ikke bare Russland, men også Kina, Iran og Pakistan er store utfordringer når det gjelder etterretning i Norge. Ønsket om å skaffe seg varer og teknologi fra diverse norske aktører er stor, der denne teknologien brukes til militær utvikling (PST, 2023, s.4)

Med stadig større informasjonsflyt og et samfunn som bryr seg om miljøet kan miljøaktivisme utgjøre en reell trussel for maritim virksomhet. Da spesielt med tanke på offshorevirksomhet
Som PST sier *"Vår vurdering er likevel at klima, miljø og naturvernsaker har et potensial til å radikalisere."*
Stort sett har miljøaktivisme i Norge gått fredelig for seg, og det finnes flere tilfeller hvor aktivistene oppnår det de ønsker ved bruk av fredelige midler . Det finnes også eksempler hvor dette ikke er tilfellet, hvor det har gått så langt at for eksempel fartøy har blitt forsøkt senket. Det skjedde for eksempel med hvalfangstskuta Skarbakk, som ble senket til kai i lofoten av klimaaktivister. (*Sabotasje Mot Hvalskute I Svolvær – NRK Norge – Oversikt Over Nyheter Fra Ulike Deler Av Landet*, 2010) Klimaaktivisme byr altså også på utfordringer for sikkerheten til fartøy.

1.2 AKTUALITET

For å danne en sammensetning og forståelse av hva som har vært og hva som er, er vi nødt til å se litt på aktuelle hendelser og videre på fremtidige mulige hendelser.
Vi kjenner alle til 9/11 som tidligere nevnt, men to maritime terrorhandlinger som har fått store konsekvenser, var bombingen av USS Cole og MV Limburg. Disse handlingene var også bidragsytere til ISPS-koden. I år 2000 ble marinefartøyet USS Cole angrepet av to selvmordsbombere. Terroraksjonen fant sted i Adenbukta som befinner seg i Jemen, der skipet skulle utføre en planlagt bunkring. Detonasjonen av eksplosivene skjedde slik at det var to selvmordsbombere som lastet en liten båt med eksplosiver, for å så kjøre midtskips langs USS Cole å detonere. (*FBI*, 2023.)

Videre så har vi også angrepet mot MV/ Limburg i 2002. Angrepet fant sted mens fartøyet fraktet olje mellom Iran og Malaysia. Det var også i dette tilfellet en selvmordsbomber som kjørte inn i skipet med eksplosiver. Det endte med at 90.000 fat olje gikk tapt og lekket ut i

Aden Gulfen. En person omkom i denne handlingen samtidig som at tolv stykker ble hardt skadet. (*BBC NEWS,* 2002)

Det har de siste årene vært en økt aktivitet med ukjente droner i Norge opp mot kritisk infrastruktur som forsvarets øvelser, installasjoner og utstyr. (*PST, 2018*). I tillegg kan det for eksempel festes eksplosiver, eller andre innretninger til droner. Dette ser vi at dronene blir brukt til i andre land. En drone er ikke lett å oppdage på grunn av sin størrelse, og fungerer dermed utmerket til overvåkning og sabotasje.

Vi ser at norsk teknologi er interessant for andre stater. PST vurderer det som svært sannsynlig at det vil bli forsøkt innhentet informasjon om norsk teknologi, et av feltene som er av interesse er maritim teknologi ved selvkjørende skip. Dette kan bli forsøkt innhentet ved for eksempel dataangrep.
Oppkjøp er en problematikk det fokuseres stadig mer på. Det vil da være ønskelig for fremmede stater å kjøpe seg inn eller kjøpe opp norske bedrifter. Disse bedriftene kan supplere til nasjonalt viktig infrastruktur eller som tidligere nevnt, ny teknologi. Et godt eksempel på dette er at Bergen Engines nesten ble kjøpt opp av russiske interesser, der Bergen Engines leverte kritisk materiell til amerikanske og norske fregatter.

Klimaaktivisme, "*personer som arbeider aktivt for å skape oppmerksomhet om klimaspørsmål"* (NAOB, 2023)er et begrep som stadig får fokus da spesielt i sammenheng med oljevirksomhet og utgjør også en naturlig del av en sårbarhetsvurdering i de tilfellene hvor dette kan være et risikomoment.

I april 2019, tok 4 miljøaktivister seg ombord på plattformen West Hercules. Grunnen til bordingen av oljeriggen var nemlig at organisasjonen Greenpeace, som disse miljøaktivistene var medlem av, ville gjennomføre en ikkevoldelig protest mot boring etter olje og gass i Barentshavet. Lederen av Greenpeace Frode Pleym kom med et slikt svar som at det å bore etter olje i Arktis er helt helt galskap. Hvertfall når Arktis nå smelter fortere enn noensinne. Videre argumenterer Greenpeace Norge med at om oljeriggen West Hercules da skal opp og bore etter olje i det nordligste oljefeltet i verden, så ender det med at målene i Parisavtalen ikke kommer til å bli nådd. (Vissgren et al., 2019)

Tidlig 2023, fikk verftet Aibel i Haugesund en vedlikeholdskontrakt på FPSOen (Floating Production Storage and Offloading) Penguin ,som er et flytende fartøy som produserer olje til havs, eid av Shell. Under frakt til verftet i Haugesund tok klimaaktivister seg ombord i fartøyet White Marlin som sto for frakten, for å protestere mot oljevirksomhet. Protestene gikk fredelig for seg, og aktivistene ble med på ferden til Haugesund hvor de gikk i land.

1.3 PROBLEMSTILLING

Som innledningsvis diskutert står vi overfor en ny sikkerhetspolitisk situasjon i Norge i dag. Vi har da valgt å ta for oss problemstillingen:

> *Hva ligger i skipssikkerhetsforskriftens (og ISPS-kodens) krav om at det må gjøres en sårbarhetsvurdering for skip – særlig med tanke på tankbåter i norske farvann i lys av dagens utfordrende sikkerhetspolitiske situasjon?*

Ved å svare på problemstillingen ønsker vi å oppklare hva som ligger i begrepet sårbarhetsvurdering og hvilke regler som presiserer dette og ikke minst hva regelverket krever,

1.4 AVGRENSNING

Området vi da har valgt å utforske har et stort omfang, der det er viktig å presisere hva vi ønsker å holde oss til.
Vi begrenser oss til maskindrevne næringsdrivende fartøy, nærmere bestemt tankskip med en bruttotonnasje på 500 og derover i norske farvann. Vi kommer ikke til å ta høyde for statlige, fritidsfartøy og andre fartøy som ikke driver sivil næring. Vi vil bruke norske lover som fokuserer på sårbarhetsvurdering, herunder skipssikkerhetsloven og sikkerhetsforskriften. Regelverkene omhandler også havneanlegg, noe vi ikke vil ta stilling til i denne oppgaven. De norske lovene vil vise til ISPS koden, som er et internasjonalt regelverk fra IMO som gjennomføres fra EU der Norge har innlemmet disse via EØS.

2.0 METODE

Når man ønsker å finne svar på forskningsspørsmål, er man nødt til å ta i bruk en forskningsmetode. Til vår oppgave vil vi bruke rettsvitenskapelig metode ettersom at vi i vår

oppgave utforsker hvilke lover og regler som gjelder for sårbarhetsvurdering, og hva reglene går ut på.

2.1 RETTSVITENSKAPELIG METODE

Rettsvitenskapelig metode har som mål å finne svar på rettsspørsmålet

Metoden går ut på å tolke, analysere og drøfte selve lovtekstens ordlyd, men det er her viktig å presisere at ordlyden ikke er det eneste man skal se på, det må tas hensyn til alle relevante rettskilder når et rettsspørsmål skal besvares (Simonsen, 2020, s.2)
Rettsvitenskapelig metode setter lover og regler i et system eller hierarki hvor det er 7 rettskilder man vanligvis ser på i en gitt rekkefølge:
lover og forskrifter , sedvaner, forarbeider, folkerett, rettspraksis, stats- og forvaltningspraksis, bransjepraksis og juridisk litteratur og reelle hensyn (Simonsen, 2020 s.6)

For å kunne komme fram til svar på det gjeldende rettspørsmålet må vi veie, drøfte og sammenligne de forskjellige rettskildene. Som nevnt i forrige avsnitt, vektes de forskjellige kildene forskjellig, og det er derfor viktig at dette tas høyde for i vurderingen av rettsspørsmålet. Et begrep som her er verdt å få med, er begrepet sikker juss. Dersom rettskildene trekker i samme retning og vil resultatet av analysen fremstå som sikker, er dette et begrep som heter sikker juss. Rettskilder som derimot trekker i forskjellige retninger etterlater et større rom for tolkning og ulike oppfatninger på hva regelen sier. Det kreves da at det tas større hensyn til rettskildenes vekting for å kunne svare på rettsspørsmålet (Simonsen, 2020 s.7). I vår oppgave vil det være vanskelig å vise til sikker juss, da rettskildene gir en større åpning for drøfting.

2.2 AKTUELLE RETTSKILDER

For å kunne løse en rettsvitenskapelig oppgave trenger vi rettskilder. Lovverkene nevnt i dette kapittelet danner grunnlaget vi har samlet inn til bruk i oppgaven. Vi vil i stor grad forholde oss til lover og forskrifter da emnet sårbarhetsvurdering er et felt hvor det eksisterer ingen rettspraksis. (Bull & Pettersen, 2010, s.576)

Innledningsvis kan det også være greit å definere hva sikkerhet er. Sikkerhet på norsk, dekker det som er både "security" og "safety" i det engelske språket. det er derfor nødvendig å ha et forhold til at security viser til hindring og tiltak mot angrep, mens safety heller viser til for eksempel sikringsutstyr som redningsvester og lignende. I vår oppgave er det "security," som utgjør det interessante i og med at dette inneholder sikringstiltak mot terror, sabotasje og lignende aktivitet mot fartøy.

2.2.1 SKIPSSIKKERHETSLOVEN

Først og fremst har vi Skipssikkerhetsloven. Denne trådte i kraft 2007 og erstattet sjødyktighetsloven, som hadde vært gjeldende regelverk fra 1902 frem til det ble opphevet i 2007. Loven forvaltes av nærings- og fiskeridepartementet og Sjøfartsdirektoratet og er gjeldende for alle norske og utenlandske skip som er 24 meter eller over utenfor næringsvirksomhet. Lovens formål er:

"Loven skal trygge liv og helse, miljø og materielle verdier ved å legge til rette for god skipssikkerhet og sikkerhetsstyring, herunder hindre forurensning fra skip, sikre et fullt forsvarlig arbeidsmiljø og trygge arbeidsforhold om bord på skipet, samt et godt og tidsmessig tilsyn." (Skipssikkerhetsloven, 2007, §1)

Lovens formål er altså å forhindre ulykker til sjøs, gjøre arbeidet sikrere for de som har sitt arbeid om bord på skip, sikre om materiell og verdier og forebygge forurensing. Skipssikkerhetsloven danner grunnlaget for sårbarhetsvurdering i det norske regelverket, og blir derav en naturlig del av rettskildene vi bruker i denne oppgaven. I vår oppgave kommer vi særlig til å bruke skipssikkerhetslovens §39 om forebyggende tiltak mot angrep mv. på skip.

2.2.2 SIKKERHETSFORSKRIFTEN

Sikkerhetsforskriften er hjemlet i skipssikkerhetsloven § 39 tredje ledd og er vesentlig for sårbarhetsvurdering og presiserer skipssikkerhetsloven særlig med tanke på sårbarhetsvurdering. Den heter da i sitt fulle navn:

"Forskrift om sikkerhet, pirat- og terrorberedskapstiltak og bruk av maktmidler om bord på skip og flyttbare boreinnretninger"

Forskriften trådte i kraft i 2004 og gjennomfører ISPS-koden i norsk rett. Forskriftens formål er å sikre skip som ferdes på sjøen med sikkerhet mot de trusler som kan være relevante for skip. Dette er i hovedsak forskriften vi kommer til å benytte, ettersom at det er denne som gir føringer for hva en sårbarhetsvurdering skal inneholde. §8 er sentral for sårbarhetsvurdering.

2.2.3 INTERNASJONALE LOVVERK

Som nevnt innledningsvis dannet IMO etter 9/11 raskt et regelverk som er aktuelt for vår oppgave.

"IMO – International Maritime Organization – er FNs særorganisasjon med ansvar for sikkerhet og skipsfart og forebygging av marin og atmosfærisk forurensning fra skip. "IMOs arbeid støtter FNs bærekraftsmål." (IMO, 2023)

Videre har IMO konvensjonen SOLAS (Safety of life at sea). Denne er ansett som den viktigste av konvensjonene som regulerer sikkerhet for næringsdrivende skip. De første utgivelsene daterer tilbake til 1914 og kom som en direkte respons til Titanic-ulykken. For vår oppgave er kapittel XI-2 som har tittelen "*Special measures to enhance maritime security"* vesentlig. Her ligger ISPS koden som fastsetter krav og veiledninger til hva som bør utføres, påtenkes og vurderes i forhold til sikkerhet. Denne koden er innlemmet i Norsk rett via forordning fra EØS.

2.2.4 LOVFORARBEID

Etter å ha sett på norske og internasjonale forskrifter, blir det naturlig å analysere forarbeidene til loven. For at en lov skal bli til, må det gjøres et grundig arbeid i forkant. De som utarbeider lovforarbeidet må da ta stilling til hvorfor denne loven skal inn i norsk rett og hva den handler om. Lovforarbeidet er dermed en av de viktigste rettskildene vi har til å tolke loven. Forarbeidet til skipssikkerhetsloven §39 er gjort ut fra ot.prp.(odelstingsproposisjon) nr. 87 fra 2005 og NOU (Norges offentlige utredninger) 14 fra 2005. Altså utredninger gjort av staten med et saklig utvalg.

2.2.5 FORVALTNINGSPRAKSIS

Forvaltningspraksis viser til den praksisen som utøves av for eksempel departementer eller direktorater. I vårt tilfelle er det Sjøfartsdirektoratet som forvalter regelverket som omhandler sårbarhetsvurdering.

Sjøfartsdirektoratet arbeider også med anerkjente klasseselskaper for å gjennomgå og godkjenne sikkerhetsplaner slik at sikkerhetsplanene kan bli godkjent innen en rimelig tid. Disse selskapene med Sjøfartsdirektoratet er klassifikasjonsselskap eller kalt klasseselskap. Et eksempel på dette er DNV (Den Norske Veritas) som er et av Norges eldste klasseselskap. (Simonsen, 2022, s.327)
Sikkerhetsforskriften belyser også dette ved §9
"(3) Innholdet i fartøyets sikkerhets- og terrorberedskapsplan (SSP) skal godkjennes av Sjøfartsdirektoratet eller anerkjent klasseinstitusjon (RSO)."

2.2.6 JURIDISK LITTERATUR

Det finnes noen bøker som har noe relevant til problemstillingen vår, disse har vi valgt å bruke. Bøkene vi hovedsakelig benytter er Skipssikkerhetsrett (Simonsen, 2022), Security at Sea (Kopperud & Askildt, 2003.), Skipssikkerhetsloven med kommentarer (Bull & Pettersen, 2010) og sjørett (Falkanger & Bull, 2010)

Et formelt søk etter litteratur går ut på å søke i databaser med forskningsrelaterte tekster. Til dette har vi hovedsakelig brukt Oria.no der følgende søkeord er brukt:

SØKEORD	Treff
ISPS CODE	**773**
ISPS CODE IN NORWEGIAN SEA	**2**

ISPS KODEN I NORGE	**0**
SÅRBARHETSVURDERING I NORGE	**0**
SHIP SECURITY ASSESSMENT	**610**
SÅRBARHETSVURDERING	**6**
BEREDSKAPSPLAN	**10**
SHIP SECURITY PLAN	**547**
SHIP SECURITY ASSESSMENT IN NORWAY	**0**

Vi har hatt et formelt litteratursøk og søkt med de spesifikke søkeordene som står ovenfor. På de mest generelle søkeordene har det naturlig dukket opp mange treff, og som vi tidligere har skrevet, så er det lite litteratur som går inn på problemstillingen vår som går helt spesifikt på sårbarhetsvurdering. Derimot det vi kunne få bruk for i oppgaven vår var boka (Security at sea) (Kopperud & Askildt, 2003).

Som vi ser, er det lite som omfatter vår problemstilling. Dette er da også en nettopp en av grunnene til at vi ønsker å skrive denne bacheloren for å belyse dette uutforskede temaet.

3.0 SÅRBARHETSVURDERING

For å finne svar på problemstillingen vår:

> *Hva ligger i skipssikkerhetsforskriftens (og ISPS-kodens) krav om at det må gjøres en sårbarhetsvurdering for skip – særlig med tanke på tankbåter i norske farvann i lys av dagens utfordrende sikkerhetspolitiske situasjon?*

Det er naturlig å først få et innblikk i hva en sårbarhetsvurdering er, og hva den skal inneholde. Videre skal vi tolke, analysere og drøfte ordlyden til lover og regler fastsatt av den norske stat.

Hva er så en sårbarhetsvurdering?
Sikkerhetsforskriftens definerer dette ved §2 bokstav y, som gir følgende definisjon:

"Sårbarhetsvurdering (Ship security assessment, SSA): Vurdering med hensyn til sårbarhet for terroranslag mot fartøy."

Terroranslag eller terrorhandling er definert ved Lov om forebyggende sikkerhetstjeneste §3,

"5. Terrorhandlinger; 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."

Som vi ser fra ordlyden vil dette dekke et bredt spekter av ulovlige handlinger, men i forarbeidet til skipssikkerhetsloven er terrorhandlinger definert ved *"situasjoner der en eller flere representanter for en terrorgruppe eller lignende truer eller iverksetter handlinger."* (Bull & Pettersen, 2010, s. 580).

Men en sårbarhetsvurdering vil uansett dekke et bredt spekter, der vurderinger mot terroranslag vil påvirke tiltak mot andre ulovlige handlinger.

I vår bacheloroppgave legger vi vekt på viktigheten bak det å ha en sårbarhetsvurdering for utsatte mål som da er for vår problemstilling, tankskip, og vi vil da legge vekt på hvordan og

hvilke tiltak som kan hjelpe til for å eventuelt være forberedt på eventuelle sikkerhetsutfordringer.

3.1 SKIPSSIKKERHETSLOVEN §39

For å få svar på problemstillingen vår må vi først se på hvor kravet om sårbarhetsvurdering kommer fra. Dette kravet finnes i skipssikkerhetslovens §39.

Som tidligere nevnt er skipssikkerhetsloven sentral, og det er dette lovverket som pålegger en sårbarhetsvurdering. Loven inneholder 3 ledd og danner grunnlaget for sårbarhetsanalysen. I hovedsak tar vi til rette for første og tredje ledd der dette vil omhandle sårbarhetsvurdering.

Videre er virkeområdet til loven gitt fra skipssikkerhetslovens §2 *"Loven får anvendelse for norske og utenlandske skip. For skip under 24 meter største lengde som brukes utenfor næringsvirksomhet, gjelder loven likevel ikke."* Loven gjelder da for alle skip unntatt fritidsbåter under 24 meter.

3.1.1 FØRSTE LEDD

For å forstå omfanget av paragraf 39 er vi nødt til å se på og ta utgangspunkt i ordlyden.

"Det skal treffes tiltak for å hindre og beskytte skipet mot terrorhandlinger, piratvirksomhet, blindpassasjerer og andre ulovlige handlinger."

For å utarbeide sikkerhetstiltak som vil være til hinder og beskyttelse mot ulovlige handlinger så må det først identifiseres og vurderes for hva det skal beskyttes mot og hva som trenger beskyttelse. Skipet i seg selv skal beskyttes, men et skip består av flere elementer med ulike sårbarheter. Dermed så må det utarbeides en sårbarhetsvurdering. Og da kan "*treffes tiltak*" i så måte også ses på som en sårbarhetsvurdering.
Lovteksten er veldig presis med bruk av terrorhandlinger, piratvirksomhet og blindpassasjerer, men samtidig brukes "*andre ulovlige handlinger*" som en sekkeform (ot.prp. nr 87 s.124) som vil si at dette vil omhandle et bredt spekter. Alt fra sabotasje til fyll, slåssing og lignende. (Simonsen, 2022, s.312)

Hverken terrorhandlinger, piratvirksomhet eller blindpassasjerer er et stort problem i norske farvann. Dermed ut fra "sårbarhetsanalyse for norske tankbåter i norske farvann" vil sekkeformen "Det skal treffes tiltak for å hindre og beskytte mot andre ulovlige handlinger" være det mest sentrale virkeområdet for norske farvann. Som tidligere nevnt og situasjonen i dag 2022-23 kan det tenkes at tankbåter kan være mål, utsatt for espionasje, sabotasje, digitale angrep og andre ulovlige handlinger som kan skade skipet, dets besetning og andre rundt. Dermed som sagt ovenfor er det allerede ved første ledd gitt at det er pålagt en sårbarhetsvurdering for hvert enkelt skip, dette kommer i videre presisering ved tredje ledd, der forskrift er gitt for sårbarhetsvurdering.

3.1.2 TREDJE LEDD

For å få klarhet i hva som vil inngå i presiseringen, er det naturlig å se på tredje ledd, hvor det står:

"Departementet kan gi forskrifter med nærmere bestemmelser om kravene til sikkerhets- og terrorberedskapen på skip, herunder om:

a. hvilke skip som skal være omfattet av reglene,
b. plikt til å foreta en sårbarhetsvurdering,
c. plikt til å ha en godkjent sikkerhets- og terrorberedskapsplan for skipet,
d. plikt til å utpeke og lære opp særskilt personell med ansvar for sikkerhets- og terrorberedskap på skipet og i rederiet,
e. terroralarmsystem på skipet,
f. kontroll av personer og gjenstander som er eller skal om bord på skipet,
g. utstedelse og utforming av identifikasjonsbevis,
h. sikkerhets- og terrorberedskapssertifikater."

Som vi ser fra ordlyden så kan departementet gi forskrifter med nærmere bestemmelser. I henhold til vår problemstilling ser vi at bokstav b. "*plikt til å foreta en sårbarhetsvurdering,"* er særdeles relevant. Og under dette punktet vil sikkerhetsforskriften være den sentrale forskriften som er gitt av departementet. Forskriften vil da bidra til en presisering av skipssikkerhetsloven § 39 der som tidligere nevnt ved første ledd; "treffes tiltak for å hindre ulovlige handlinger kan i så måte ses på som en sårbarhetsvurdering"

3.2 SIKKERHETSFORSKRIFTEN

Videre blir det naturlig å se på sikkerhetsforskriften, da den presiserer det som står i loven. Som nevnt, så er det tredje del fra SSL § 39 som presiserer.

Som skrevet under undertittelen skipssikkerhetsloven så er virkeområdet gjeldende for alle skip over 24 meter. Derimot så har sikkerhetsforskriften et eget virkeområde som belyst nedenfor, jf. sikkerhetsforskriften § 1;

a. Passasjerskip, herunder hurtiggående passasjerskip, som er sertifisert for internasjonal fart som definert i SOLAS kap. I, regel 2(d), samt passasjerskip som er sertifisert for passasjerskipsklasse A som definert i den til enhver tid gjeldende forskrift om besiktelse, bygging og utrustning av passasjerskip i innenriksfart;

b. lasteskip, herunder hurtiggående lasteskip, med bruttotonnasje på 500 og derover, som er sertifisert for internasjonal fart som definert i SOLAS kap. I, regel 2(d);

c. flyttbare boreinnretninger. Flyttbare boreinnretninger omfattes likevel ikke av kravene i denne forskrift når de er på lokasjon eller hvis de ikke forflytter seg utenfor norske jurisdiksjonsområder"

Om vi ser på bokstav b, er det en avgrensing der forskriften gjelder for lasteskip med en bruttotonnasje på 500 og derover. Det vil si at for lasteskip med bruttotonnasje under dette gjelder forskriften likevel ikke. Definisjonen på lasteskip er som følger jf. sikkerhetsforskriften § 2 bokstav p: "*Lasteskip: Ethvert skip som ikke er passasjerskip, fiske- og fangstfartøy, lekter, fritidsfartøy eller flyttbar innretning."* I og med at vi har avgrenset oss til tankskip vil dette gjelde for oss. Vi har da valgt å forholde oss til tankskip med en bruttotonnasje på over 500.

3.2.1 PLIKTER OG ANSVAR

I dette delkapitlet vil vi se på hvem som har plikt og ansvar det er da naturlig se på skipssikkerhetsloven. jf. skipssikkerhetslovens § 6 andre ledd pålegger rederiet det overordnede ansvaret:

"Rederiet skal sørge for at lovens krav oppfylles, bortsett fra i tilfelle der skipsføreren i loven er gitt en selvstendig plikt til å sørge for dette."Rederiet skal sørge for at forholdene legges til rette for at alle de som har sitt arbeid om bord, har mulighet for å oppfylle sine forpliktelser etter loven.

Av ordlyden ser vi at rederiet pålegges ansvaret for at lovens krav oppfylles, som for en sårbarhetsvurdering vil være § 39. Unntaket er i de tilfellene hvor skipsfører gjennom lovverket gis ansvar. Men loven sier ikke noe om skipsførerens plikter etter §39. altså har rederiet både påse ansvaret og sørge for ansvaret. Videre pålegges rederiet å legge til rette for at de som arbeider ombord har anledning til å oppfylle det som forventes av dem i loven.

Videre utdypes ansvaret jf. sikkerhetsforskriftens §3. Her pålegges "*Rederiet, skipsføreren og andre som har sitt arbeid om bord,"* å følge plikter som gis av skipssikkerhetsloven med utfyllende bestemmelser.

Det er vanlig at en del av ansvaret som tildeles rederiet tilfaller rederiets sikkerhets-og terrorberedskapsoffiser (CSO - company security officer.) Sikkerhetsforskriftens §14 første ledd pålegger rederiet å ha en sikkerhets-og terrorberedskapsoffiser som har som oppgave å følge opp rederiets plikter i forhold til gjeldende regelverk og norm. Sikkerhetsforskriftens §2 bokstav U gir følgende definisjon:

"Rederiets sikkerhets- og terrorberedsskapsoffiser (Company Security Officer, CSO): Person som er oppnevnt av fartøyets rederi til å sørge for at sårbarhetsvurderinger er utført, at SSP er utarbeidet, innsendt for godkjennelse og deretter implementert, fulgt og vedlikehold. "CSO er også kontaktperson til PFSO og SSO."

Det er også viktig å bemerke at selv om rederiets sikkerhetsoffiser gis et personlig ansvar, er det fortsatt rederiet som har det overordnede ansvaret, jf. Lovens §6. (Simonsen, 2022, S.315)

3.2.2 SIKKERHETSFORSKRIFTEN § 5

For å danne en forståelse for hvordan internasjonale og norske regelverk samvirker, må vi se på sikkerhetsforskriftens §5. Dette er en av forskriftene vi kommer til å bruke for å forstå hvilke regler som er gjeldende for ISPS-koden.

"Fartøy som omfattes av denne forskrift skal følge de relevante kravene i SOLAS kap. XI-1, regel 3 og 5, kap. XI-2 samt ISPS-kodens del A. ISPS-kodens del B er veiledende retningslinjer som det skal tas hensyn til i det omfang del A bestemmer det, med unntak av følgende deler av del B som er bindende; 1.12, 1.16, 4.1, 4.4, 4.5, 4.8, 4.14, 4.15, 4.16, 4.18, 4.24, 4.28, 4.41, 4.45, 6.1, 8.3 til 8.10, 9.2, 9.4, 13.6 og 13.7"

Forskriften er veldig klar på hva som er gjeldende rett med tanke på ISPS koden. Kapittel XI-2 som da inneholder ISPS koden med videre presisering på at del A er gjeldende og Del B er veiledende. Som vi ser fra forskriften så er det et unntak, der deler av del B blir bindende i norsk rett. Altså gjeldende rett. For sårbarhetsvurdering er dette 8.3-8.10 som vi vil gå nærmere innpå senere.

3.2.3 § 6. FORHOLDET TIL EU REGELVERK

Videre er vi nødt til å se på §6 der EU har pålagt Norge å følge sine bestemmelser. Dette er da gitt fra EØS-avtalen.

"EØS-avtalen vedlegg XIII nr. 56bb (Europaparlamentets- og rådsforordning (EF) nr. 725/2004 av 31. mars 2004 om styrket sikring av skip og havneanlegg), gjelder som forskrift med de tilpasninger som følger av vedlegg XIII, protokoll 1 til avtalen og avtalen for øvrig. Det vises til vedlegg 1 i forskriften. Ved eventuell konflikt mellom øvrige bestemmelser i forskriften og ovennevnte forordning, har sistnevnte forrang"

Det vil si at forordningen vedlagt ved denne forskriften er gjeldende rett, der vedlegget er så å si en direkte implementering av ISPS koden.

"*EUs regelproduksjon er på et punkt spesielt. Der EUs regelverk er kommet til uttrykk i forordninger, må regelverket gjennomføres ordrett. Forordningens innhold kan altså ikke gjengis i vanlig norsk lov eller forskriftsform.*" (*NOU 2005: 14*.)

Det er verdt å få med seg at *"Forordningens innhold kan altså ikke gjengis i vanlig norsk lov eller forskriftsform.*" Dette betyr at vi ikke kan lage vår egen norske versjon, men heller må nøye oss med å oversette til norsk.

3.2.4 SIKKERHETSFORSKRIFT § 8

Som vi ser over så er det allerede fastsatt fra sikkerhetsforskriften §5 og §6 at ISPS koden er bindende. Dette vil da si at sårbarhetsvurdering som er en vesentlig del av ISPS koden er bindende. Sikkerhetsforskriften velger også å belyse dette ved egen regel,

"(1) Det skal utarbeides en sårbarhetsvurdering som beskrevet i ISPS-kodens del A, seksjon 8."

Ser vi på helheten av sikkerhetsforskriften § 8, så ser vi at ordlyden her er veldig presis og rett frem. Der det henvises direkte til det spesifikke kapittelet som omhandler sårbarhetsvurdering i del A.
Videre presiserer §8 grunnlaget for sårbarhetsvurderingen

"(2) Sårbarhetsvurderingen skal danne grunnlag for å utarbeide og oppdatere sikkerhets- og terrorberedskapsplanen."

Med et stadig endrende bilde av trusselsituasjonen vil tiltak måtte oppdateres. Dette belyses her ved at sårbarhetsvurderingen skal være fullstendig slik at om situasjonen skulle endre seg er grunnarbeidet lagt. Dette er videre presisert ved §9,
"(1) Det skal utarbeides en sikkerhets- og terrorberedskapsplan på grunnlag av sårbarhetsvurderingen (SSA), jf. § 8. Fartøyets sikkerhets- og terrorberedskapsplan (SSP) skal utformes, oppbevares og endres i henhold til ISPS-kodens del A, seksjon 9."

3.3 ISPS KODEN

Som nevnt innledningsvis gir ISPS-koden retningslinjer for hvordan en sårbarhetsvurdering skal utføres. Vi vil derfor gå gjennom hvert enkelt punkt for å skape en klarhet i hva de ulike punktene handler om.
Isps koden er både gjeldende rett og en veiledning til sårbarhetsvurdering, hvor kapittel 8 handler om sårbarhetsvurdering. ISPS koden er delt opp i to deler, med en del A for gjeldende regler og en del B med veiledende.

"At a closed-door meeting in an advisory board in the administration of ISPS Code under the TBST, the chairman stated: *"when there has been an accident, there is too little security, but when nothing happens, there is too much ".* (J. Dalgaard, 2021, s.11) Der denne uttalelsen fenger og belyser litt det samme vi kan tenke oss som skjer i Norge. Det føles gjerne unødvendig med sårbarhetsvurdering og sikkerhetstiltak, frem til dagen hvor hendelsen skjer og det utenkelige er blitt realitet.

Som tidligere skrevet vil vi tolke, analysere og drøfte hvert punkt som er gjeldende rett. Dette er Del A med fem punkter og Del B fra punktet 8.3 til og med 8.10.

I dette kapitlet eksisterer det lite rettskilder og litteratur vi kan basere oss på. Vi har derfor i liten grad andre rettskilder å forholde oss til annet enn selve ISPS-koden.

3.3.3 ISPS DEL A

Del A, som nevnt ovenfor består av fem punkter som er gjeldende rett. jf. sikkerhetsforskriften §5 første punkt står det "*Sårbarhetsvurderingen av et fartøy er en vesentlig og integrert del av prosessen med å utarbeide og ajourføre fartøyets sikkerhetsplan*."(8.1). Altså så er sårbarhetsvurderingen en av de viktigste prosessene til sikkerhetsplanen som brukes for å holde en tilfredsstillende sikkerhet ombord. Det er viktig å merke seg ordlyden *ajourføre,* der dette vil tilsi at det kreves at sikkerhetsplanen oppdateres kontinuerlig ved oppdateringer til sårbarhetsvurderingen. Det vil også være nødvendig å oppdatere sårbarhetsvurderingen ved endringer i trusselbildet. Som skrevet innledningsvis leverer PST, NSM og E-tjenesten ut rapporter for trusselvurdering.

Videre ved punkt 8.2 står det at "*Rederiets sikkerhetsoffiser skal sørge for at sårbarhetsvurderingen av fartøyet utføres av personer med tilstrekkelige kvalifikasjoner til å vurdere sikkerheten for et fartøy, i samsvar med dette avsnittet, samtidig som det tas hensyn til veiledningen som gis i del B av dette regelverket*." Dette vil for det første si at rederiet har til ansvar og fremstille en sårbarhetsvurdering. Nærmere spesifisert så er det sikkerhetsoffiseren som tillegges dette ansvaret innenfor rederiet. Videre så er det sikkerhetsoffiseren som på vegne av rederiet skal påse at det er kvalifiserte personer som utarbeider sårbarhetsvurderingen. Sårbarhetsvurderingen skal også samsvare og følge reglene fra dette avsnittet, altså avsnitt 8. Det tolkes også som del B skal brukes aktivt for å vurdere sårbarhetsvurderingen, der "tas hensyn til" viser til del B som veiledende.

Andre enn selve rederiet kan utføre selve sårbarhetsvurderingen, men det er rederiet som har ansvaret. "*Med forbehold for bestemmelsene i avsnitt 9.2.1, kan en anerkjent sikkerhetsorganisasjon utføre sårbarhetsvurderingen av et bestemt fartøy"* (8.3).
Avsnitt 9.2.1 lyder da følgende:
"I slike tilfeller skal den anerkjente sikkerhetsorganisasjonen som gjennomfører gjennomgåelsen og godkjenningen av en sikkerhetsplan for et bestemt fartøy, eller endringer av den, ikke ha vært involvert i verken sårbarhetsvurderingen av fartøyet eller utarbeidingen eller endringer av den sikkerhetsplanen som gjennomgås." (9.2.1). Det vil si at Sjøfartsdirektoratet og/eller med klasseselskap/klassifikasjonsselskap som gjennomgår og godkjenner en sikkerhetsplan, ikke kan bidra til hverken sårbarhetsvurderingen eller sikkerhetsplanen når den utarbeides. Derimot om en av disse ikke er med på godkjenningen, kan de være med å utarbeide sårbarhetsvurderingen.

Videre heter det i ISPS kodens del A punkt 8.4; "*Sårbarhetsvurderingen av et fartøy skal omfatte sikkerhetsundersøkelse på stedet, og minst følgende elementer:"*
Ordlyden fra første ledd til komma, sier for det første at en sikkerhetsundersøkelse skal finne sted, men også at det skal gjøres på selve fartøyet. Andre ledd presiserer hvor omfattende den *minst* skal være på fartøyet. Altså minimumskrav til sikkerhetsundersøkelsen på selve fartøyet. Minimumskrav er i denne forstand krav som *skal* gjennomføres, men rederiet må gjerne gjøre mer.

Det første punktet viser til: "*identifisering av eksisterende sikkerhetstiltak, -framgangsmåter og -virksomhet*". På selve fartøyet skal det da foretas en identifisering av hvilke tiltak som allerede eksisterer. Ordlyden *sikkerhetstiltak* dekker et stort omfang, det samme gjelder *fremgangsmåter og virksomhet*. Det å identifisere iverksatte tiltak er viktig slik at ikke eventuelle nye tiltak som utarbeides skaper en sikkerhets konflikt. Statlige aktører vet å utnytte sikkerhetshullene som eventuelt skulle oppstå ved en sikkerhets konflikt. Dette kan brukes til kartlegging og bli en del av de sammensatte truslene.

Det er da viktig å se på ordlydens opprinnelige språk for å presisere i dette tilfellet, der det brukes "security" og ikke "safety". Forarbeidet og den gjennomgående konteksten vil også belyse dette, der sikkerhet i denne forstand er beskyttelse mot og tiltak for å hindre angrep. Det er derfor viktig å presisere sikkerhet i det norske språket.

"identifisering og vurdering av vesentlige funksjoner om bord som det er viktig å beskytte"
Andre punkt bestemmer at det skal identifiseres og vurderes hvilke funksjoner som er vesentlige, altså viktige funksjoner som brukes regelmessig om bord og trenger å beskyttes. Dette kan være for eksempel nettverket ombord. Sårbarhetsvurderingen må da presisere enkeltmomenter som er viktige å beskytte. Tankbåter har mange vesentlige funksjoner for å kunne operere, en av de vesentlige funksjonene er radiokommunikasjonen. Om denne skulle blitt "jammet", en forstyrrelse på signalet innad og utad slik at kommunikasjonen hverken kommer inn eller ut, kan dette skape problemer ute i Norskehavet. Det er sjeldent at radiokommunikasjonen er nede, men det hender at GPS signalet er nede lenger nord i landet. Dette kan tenkes at utføres av Russland. (Strøm, S. 2023)

"identifisering av mulige trusler mot vesentlige funksjoner om bord og sannsynligheten for at de skal oppstå, med det formål å fastsette og prioritere sikkerhetstiltakene,"
Tredje punkt bruker ordlyden *mulige trusler mot vesentlige funksjoner*, der mulige trusler er et vidt begrep som dekker et stort omfang. Vesentlige funksjoner er mer presist der dette viser til forrige punkt der disse funksjonene skal identifiseres. Videre skal det gjøres en redegjørelse for sannsynligheten for at disse *mulige truslene* inntreffer. Slik at det både er en forståelse for hva som kan gå galt og for å *fastsette og prioritere sikkerhetstiltakene*.
En mulig trussel mot tankbåter er angrep på data- eller nettverkssystemer, der angrepet kan brukes til mangt. Ut fra PST trusselvurdering er nok kartlegging i første omgang det ønskelige målet, men ved tilgang til datasystemet ombord er det mye informasjon som kan

hentes. Viktige dokumenter, fremtidige planer og personlig informasjon er bare noe av det som kan være lagret ombord i systemet.

"Identifisering av svakheter, herunder menneskelige faktorer, i infrastrukturen, politikken og framgangsmåtene"
Fjerde punkt handler om å identifisere de svakheter fartøyet har med tanke på sikkerhet. Med en videre presisering, altså i tillegg, på menneskelige faktorer, infrastrukturen, politikken (retningslinjer), og fremgangsmåtene.
Menneskelige faktorer har i all tid kunne bli utnyttet, der ønsket om bedre økonomi eller rett og slett utpressing ofte er midler som brukes for å legge press på individer. I norske farvann kan også dette være en realitet der individer i besetningen kanskje ønsker seg litt mer penger. Det å rekruttere nøkkelpersoner til etterretning eller til sabotering av egen bedrift kan absolutt være ønskelig fra statlige aktører.

"Fartøyets sårbarhetsvurdering skal dokumenteres, gjennomgås, godtas og oppbevares av rederiet"
Altså det vil si at rederiet er den ansvarlige, som tidligere nevnt, for sårbarhetsvurderingen. Det vi ser fra del A fra ISPS-koden er hvem som har ansvaret for at dette gjøres, dokumenteres, gjennomgås og oppbevares. Dette skal så leveres med sikkerhetsplanen til de som godkjenner slik at vurderingen for tiltakene belyses.

Som vi ser så er del A generelt dekkende for en sårbarhetsvurdering, der ordlyden dekker et stort omfang. I tillegg til bruk av del B av ISPS koden, som det allerede tilsier at bør brukes, vil omfanget presiseres. Vi vil da gå i dybden på del B.

3.3.4 ISPS DEL B

Som tidligere nevnt har vi både EU direktiv 725/2004 som forordning, altså bindende forskrift, og en presisering i sikkerhetsforskriften. Presiseringen gjelder fra punkt 8.3 til 8.10. Disse beskriver detaljert hva som skal være med i en sårbarhetsvurdering. Dette blir da minimumskravene som må utarbeides av fagpersonell og/eller sikkerhetsoffiser for en bakgrunn til beredskapsplanen. For å få en god forståelse for hva sårbarhetsvurderingen til tankskip skal inneholde vil disse være de viktigste momentene. Vi vil derfor prøve å gå inn i detalj med hensyn til tolkning, analysering og drøfting av lovteksten.

8.3 ELEMENTER TIL SÅRBARHETSVURDERING

Det første punktet som må tas hensyn til som er bindende er 8.3. En av de mest sentrale punktene innen del B for sårbarhetsvurdering på grunn av sitt omfang. Dette lyder som følger

"En sårbarhetsvurdering av et fartøy skal ta for seg følgende elementer om bord på eller i fartøyet:
.1 fysisk sikkerhet,
.2 strukturell integritet,
.3 system for beskyttelse av personell,
.4 generelle fremgangsmåter,
.5 radio- og telekommunikasjonssystemer, herunder datasystemer og nettverk, og
.6 andre områder som kan utgjøre en risiko for personer, eiendom eller virksomhet om bord på fartøyet eller i havneanlegget dersom de skades eller brukes til ulovlig observasjon"

Som sagt er dette det første punktet fra ISPS koden del B som er bindende jf. sikkerhetsforskriften §5. Regelen presiserer da hvilke elementer som skal være med i en sårbarhetsvurdering. Og der ordlyden bruker "om bord eller i fartøyet" som også er en videreføring av del A 8.4 første setning frem til komma. "*Sårbarhetsvurderingen av et fartøy skal omfatte sikkerhetsundersøkelse på stedet"*.

Det første elementet er *fysisk sikkerhet*, der det skal vurderes for blant annet barrierer som fartøyet bør ta i bruk eller allerede brukes for å hindre adgang til for eksempel uvedkommende. Videre er det strukturell integritet som skal tas hensyn til, der fartøy er forskjellig konstruert, vil det være forskjellige sammensatte strukturer. Dette presiserer også viktigheten med at det skal være en sårbarhetsvurdering for hvert skip. For eksempel der individuelle strukturelle "skavanker" kan utnyttes for å få tilgang eller ødelegge. Dette vil også kunne presisere det første elementet, der den fysiske sikkerheten som skal vurderes, og tas høyde for, må også sees i lys av den strukturelle integriteten.
Tredje underpunktet presiserer en vurdering for systemet for beskyttelse av personell, der det ved et angrep er viktig å ha både løsninger og barrierer for at mannskapet ikke skal nås. Citadell, eller "saferoom" er en barriere for å beskytte personell. Et rom som skal være låst

innenfra og har en forsterkende struktur for å hindre adgang. Dette er en barriere som for eksempel brukes i Guineabukta, Afrika. Dette ettersom piratvirksomheten er et stort problem og er derfor ikke like aktuelt i vår case.

Generelle fremgangsmåter kan i så måte bety en vurdering av planer og tiltak som skal gjennomføres ved både nødsituasjoner og rutinemessige operasjoner. Altså tiltak for å hindre skade på liv og materielle verdier.
Det femte elementet omhandler radio og telekommunikasjon, med også en presisering på datasystemer og nettverk. Med en stadig utvikling av teknologi både for driftssystemer og muligheter for å ta kontroll over andre systemer, vil dette være et særdeles viktig element for å hindre ulovlige handlinger (§39). Systemer blir mer sofistikerte med flere funksjoner, desto mer sofistikert og funksjonsrikt systemet er, vil det også være mer komplekst å beskytte.
Som nevnt innledningsvis viser PSTs sikkerhetsrapport til at sannsynligheten for cyberkriminalitet er høy. I stor grad fra andre nasjoner, som Kina og Russland. Ønsket om å kartlegge for egen gevinst er stor. For eksempel ved å manipulere lastecomputere til å vise ulike verdier kan dette skape økonomiske tap for rederier og videre i den grad nasjonalt. Phishing, der mailer blir sendt ut for å forsøke å manipulere, er også noe som i større grad blir mer og mer sofistikert. For eksempel ved overvåking av mailer sendt ut fra rederi til skip, kan disse stoppes eller endres før de når mottakeren. (NSM, 2023, s. 31)

Det siste elementet som skal tas hensyn til er en generalisering der ordlyden bruker “og andre områder som kan utgjøre en risiko” både for skade og observasjon. Denne sekkeformen vil dekke for både nye situasjoner og situasjoner som ikke har vært påtenkt i regelverket.

8.4 INNHENTING AV SAKKYNDIG BISTAND

Der 8.3 gir elementer med presisering til sårbarhetsvurderingen, er 8.4 en omfattende regel som tar for seg innhenting av informasjon.

“De som deltar i sårbarhetsvurderingen av et fartøy, skal kunne benytte seg av bistand fra sakkyndige når det gjelder:
.1 kunnskap om gjeldende sikkerhetstrusler og -mønstre,
.2 gjenkjenning og påvisning av våpen, farlige stoffer og innretninger,

.3 gjenkjenning uten forskjellsbehandling av kjennetegnene ved og atferdsmønstrene til personer som kan utgjøre en sikkerhetstrussel,
.4 metoder som brukes til å omgå sikkerhetstiltak,
.5 metoder som brukes til å forårsake en sikkerhetshendelse,
.6 virkningen av sprengstoff på fartøyets konstruksjon og utstyr,
.7 sikkerhet for fartøyer,
.8 forretningspraksis for kontakt mellom fartøy og havn,
.9 utarbeiding av beredskapsplaner, kriseberedskap og reaksjonstiltak,
.10 fysisk sikkerhet,
.11 radio- og telekommunikasjonssystemer, herunder datasystemer og nettverk,
.12 maskineri, og
.13 fartøys- og havnevirksomhet."

Her er det viktig å få med seg "*skal kunne benytte seg av bistand"* der ordlyden ikke pålegger den ansvarlige for sårbarhetsvurderingen å aktivt søke etter bistand fra sakkyndige. Men viser til del A punkt 8.2 der det står som følger: "*Rederiets sikkerhetsoffiser skal sørge for at sårbarhetsvurderingen av fartøyet utføres av personer med tilstrekkelige kvalifikasjoner".* Det vil da si at om kunnskapen ikke er god nok, må sakkyndige brukes. Spørsmålet blir da; hva som er tilstrekkelig og godt nok.
Mye av informasjonen som kan være nyttig for sårbarhetsvurderingen når det gjelder norske farvann er nok gradert, der sikkerhetstrusler fra ekstremister og statlige aktører ofte holdes hemmelig.

Det første under-punktet handler om innhenting av kunnskap om gjeldende sikkerhetstrusler og mønstre. Trusler kan innhentes fra blant annet PSTs nasjonale trusselvurderinger rapport, men rederier har sjeldent tilgang til mer informasjon utenom dette med tanke på gradert informasjon. Eller informasjon kan hentes fra andre nasjoners sikkerhetsmyndigheter og private aktører innen dette segmentet.

Videre så skal det benyttes sakkyndige til å gi en "gjenkjenning av våpen, farlige stoffer og innretninger". Det er viktig at det vurderes hva som kan brukes til ulovlige handlinger, der det ikke alltid er like lett å identifisere dette. De fleste vil forstå at et vanlig håndvåpen kan utgjøre en trussel, men å gjenkjenne for eksempel masseødeleggelsesvåpen er ikke alltid like lett. Siden skip kan brukes som et medium til å både frakte gods til bruk av terror og til å

utføre terror eller sabotasje. I norsk sektor er det mest aktuelt med sabotasje, men det er likevel ikke utenkelig at terroraksjoner maskeres som ulykker eller terror med ønske om å fraskrive seg ansvar, da spesielt om dette skulle være statlige aktører som Russland.

Innretninger på så måte kan være for eksempel droner eller utstyr plassert ombord som kan for eksempel skade nettverk. I en stadig utviklende verden er det mange innretninger som er meget sofistikerte og i tillegg vanskelige å oppdage.

Det er heller ikke alltid like lett å kjenne igjen adferdsmønster som kjennetegner en som ønsker å volde skade. Der det å lese kroppen er et eget fagfelt i seg selv.

Det å omgå sikkerhetstiltak er blitt en stor bransje de siste årene, der det er egne selskap som tester ut sikkerhetstiltakene implementert for å finne smutthull. Disse blir ofte omtalt som "Red team". "Red Team er en gruppe ansatte i et IT-sikkerhetsselskap som utfører et kontrollert angrep på en bedrift. Angrepet er oftest digitalt, men kan også være et fysisk innbrudd, og er designet for å være " så realistisk som mulig" (Dale, C. 2020) Her vil det også være kompetanse på metoder brukt for å utløse en sikkerhetshendelse. Der dette kan brukes til å kartlegge reaksjonene både for å få en oversikt og til å eventuelt skape konflikter mellom sikkerhetstiltak. Det er tenkelig at dette kan være gunstig for tankbåter, ettersom at de absolutt de utgjøre mål for slike angrep. Det vil også bidra til å skape en bedre sårbarhetsvurdering eller i det minste oppdatere den.

Punkt 6 handler om hvordan sprengstoff vil påvirke konstruksjonen eller utstyret ombord. Der virkningen av sprengstoff på skrog som nevnt innledningsvis ved USS Cole og M/V Limburg kan få katastrofale følger. Men et skip har flere nyanser enn bare skroget, det å detonere en ladning nært et kritisk punkt på skroget kan ha større effekt enn ved detonering helt tilfeldig. Dette er det viktig å være klar over for å gjøre en god vurdering slik at sikringstiltak er presise. Det er også utstyr ombord som er kritiske, disse skal identifiseres i henhold til del A 8.4.2. Om vi ser til norske farvann kan for eksempel alt av kommunikasjonsantenner på bro taket ble slått ut av en målrettet detonasjon. For eksempel en drone med eksplosiver.
Det å gjøre en sårbarhetsvurdering for et fartøy er omfattende, der det er mange elementer som skal tas hensyn til. Det kan da ofte være en fordel å dra inn tilleggs ekspertise for å blant annet skape gode diskusjoner. Ordlyden til punkt 7 er noe upresis, der sikkerhet for fartøy er

et bredt emne. Flere av punktene vil kunne sammenfatte med denne ordlyden. I den forstand så vil den også kunne omfatte eventuelle punkt som ikke er tenkt på.
Selv om utarbeiding av sårbarhetsvurderingen gjennomføres av rederiets sikkerhetsoffiser og ofte et annet selskap dedikert til dette, kan det være en fordel å benytte seg av kunnskap utenfra om "*beredskapsplaner, kriseberedskap og reaksjons tiltak*" der det vil være en utvikling og forståelse med ny kunnskap. Videre kan det også være en fordel med kunnskap utenfra om fysisk sikkerhet der som nevnt over det er i stadig utvikling.
Et viktig punkt nå i nyere tid etter vår mening er benyttelse av sakkyndige innen "radio- og telekommunikasjon, herunder datasystemer og nettverk". Dette er et stort felt som har tatt av de siste årene. Det brukes jo flere datasystemer ombord, dette igjen skaper flere sårbare områder. Om et system er kompromittert, er det fort gjort at flere systemer er kompromitterte. I og med at det er blitt et så omfattende emne kan det absolutt være en fordel å innhente bistand fra sakkyndige for data og nettverkssikkerhet.
Maskineriet om bord er også blitt mer sofistikerte der mye styres elektronisk. Som diskutert ovenfor har data og nettverk et stort omfang og om nettverk er kompromittert kan dette utarte seg til at flere systemer kompromitteres. Om systemet for kontroll over maskineri skulle blitt infisert kan det i verste fall bli tatt over og bli brukt til f.eks. å kjøre inn i en plattform.

Som vi ser fra dette punktet, 8.4, i ISPS koden, er det lagt grundig opp til at det bør konfereres med sakkyndige for å skape en god sårbarhetsvurdering. Ordlyden bruker "skal kunne benytte seg", noe som vil føre til en individuell vurdering hos rederiets sikkerhetsoffiser om det er behov for kunnskap fra sakkyndige utenfra. Bedrifter som tilbyr utførelse av sårbarhetsvurderinger har også sakkyndige med bred kompetanse, men ofte er det fordelaktig å i tillegg benytte seg av kunnskap utenfra.

8.5 CSOENS PLIKTER

Isps-kodens 8.5 setter fokus på rederiets sikkerhetsoffiser og gir grunnlag for hvilke faktorer som skal tas høyde for i vurderingen.

"rederiets sikkerhetsoffiser skal innhente og registrere de opplysningene som er nødvendige for å foreta en vurdering, herunder:"

Som ved de tidligere reglene er også denne delt opp i en generell betydning med presiseringer for minstekrav som bør gjennomføres. 8.5 har da 13 av disse.

1. *"Fartøyets generelle utforming"*
2. *"plassering av adgangsbegrensede områder, f.eks. kommandobroen, maskinrommet i klasse A og andre kontrollstasjoner definert i kapittel II-2, osv."*
3. *"plasseringen av de faktiske eller mulige utgangspunktene til fartøyet, og deres funksjon."*
4. *"endringer i tidevannet som kan påvirke fartøyets sårbarhet eller sikkerhet."*
5. *"lasterommene og lasteplanene."*
6. *"plasseringen av skipsforsyningene og viktig vedlikeholdsutstyr."*
7. *"Plasseringen av uledsaget bagasje."*
8. *"nød- og beredskapsutstyr som er tilgjengelig for å opprettholde vesentlige tjenester"*
9. *: "besetningens størrelse, eventuelle eksisterende sikkerhetsmessige oppgaver og opplæringskrav i rederiet"* .
10. *"eksisterende sikkerhetsutstyr til beskyttelse av passasjerer og besetning"*
11. *"rømnings- og evakueringsveier og mønstringsstasjoner som skal opprettholdes for å sikre at evakuering av fartøyet foregår rolig og sikkert."*
12. *"gjeldende avtaler med private sikkerhetsselskaper som leverer sikkerhetstjenester på fartøyer og i havner, og"*
13. *"gjeldende sikkerhetstiltak og -prosedyrer, herunder framgangsmåter ved inspeksjon og kontroll, identifikasjonssystemer, overvåkingsutstyr, besetningens identifikasjonsdokumenter og kommunikasjon, alarmer, belysning, adgangskontroll og andre hensiktsmessige systemer."*

Sårbarhetsvurdering (SSA) vil være unik fra fartøy til fartøy. Det er derfor viktig at det foretas en vurdering for hvert fartøy som tar høyde for blant annet de oppdragene som skal løses, de områdene det skal opereres ol. 8.5 pålegger rederiets CSO å innhente nødvendig informasjon for å kunne foreta en vurdering.

Skipets utforming spiller stor rolle for hvorvidt skipet er sårbart, eventuelle strukturelle svakheter skipet kan ha med mer. Videre bruker regelverket ordlyden *"utgangspunktene til fartøyet"*, og her belyses det igjen at noe av meningen i koden forsvinner i implementeringen til norsk. Den originale koden viser til *"Entry points,"* (Kopperud & Askildt, 2003, S. 75)

noe som heller viser til adgangspunktene til skipet og ikke kun utgangspunktene, og dette kan igjen utgjøre en naturlig risiko.

Dersom man for eksempel skal borde et skip, vil dette enklere gjøres på skip med lavere fribord (høyde fra skuteside til vannet) og fart. Dette må også tas med i en vurdering når vi for eksempel ser på "*fartøyets generelle utforming."*. Faktorer som høy fart, manøvreringsevne og fribord vil naturlig være faktorer som gjør en kapring vanskeligere. Tankbåter kan tenkelig være aktuelle mål for kapring ettersom at dette er fartøy som beveger seg sakte, har liten manøvreringsevne og bærer store verdier. Fokuset rundt fartøy og kapring har fått et stort fokus i konfliktene rundt Afrika i nyere tid, men er ikke utenkelig i norske farvann der for eksempel russiske agenter utgi seg for å være terrorister med mål om å slå ut norsk infrastruktur. Dette kan enkelt oppnås ved eksempelvis å kjøre en tankbåt inn i en plattform.

Sårbarhetsvurderingen skal videre ta høyde for at ting kan skje selv om det ikke er veldig sannsynlig. Noe som derimot er mer sannsynlig i norsk sektor er klimaaktivister som tar seg ombord. Dette belyses gjennom den nylige aksjonen i Norskehavet hvor fartøyet "White Marlin," som nevnt innledningsvis ble bordet. Ikke-voldelige aksjoner utgjør som regel ikke fare for liv, helse eller verdier, men skaper en situasjon hvor mannskapet har mindre kontroll over fartøyet sitt. Dette skaper dog et nytt sikkerhetsmoment ombord. Hadde ønsket vært å utgjøre mer skade hadde kaprerne i dette tilfellet all mulighet til dette. Det er derfor også viktig å verne om kritisk infrastruktur ombord.

Et utsatt element for sikkerheten til skip er alt som taes ombord, fraktes eller plasseres ombord på fartøyet. Et av målene til isps-koden er at reglene og tiltakene skal forhindre at skip blir brukt til å transportere våpen, herunder masseødeleggelsesvåpen og våpendeler, farlige stoffer, anordninger, personer og lignende som kan brukes i terroraksjoner. (Simonsen, 2022, s. 309.) *"Lasterommene og lasteplanene"* ombord utgjør naturlige steder hvor slik last kan gjemmes, enten som stykkgods eller som en del som gjemmes i annen last. Dette belyses blant annet av en nylig sak med flere store kokainbeslag i norge, som sannsynligvis stammer fra sør-amerika og har ankommet gjennom terminalen rotterdam, hvor enorme mengder ulovlige stoffer har blitt smuglet i banankasser uten at dette har blitt oppdaget før produktet kom frem. Dette kunne like gjerne vært våpen eller andre farlige objekter som kunne brukes til ulovlige handlinger.

Skip er avhengig av *skipsforsyninger* og *vedlikeholdsutstyr* for å kunne operere. Dette gjør også disse til utsatte områder som skal kartlegges av skipsikkerhetsoffiser. Skipsforsyninger kan for eksempel være ting som mat og proviant til de ansatte. For en fiendtlig stat vil det være av interesse å sette norsk energiforsyning ut av drift, gjennom å lamme skipets forsyninger, vil fartøyets evne til å løse oppdrag også lammes. Det samme gjelder for vedlikeholdsutstyr som brukes for å holde fartøyet operasjonelt, hvor mangler som smøreolje, verktøy eller lignende kan føre til opphold i drift.

Videre er *"Plasseringen av uledsaget bagasje"* et moment som skal tas i sikkerhetsoffiserens betraktning. Uledsaget er bagasje som ingen ombord vedkjenner seg, og vil ved oppdagelse utgjøre et usikkerhetsmoment. Det kan her være naturlig å plassere slik bagasje en plass den eller innholdet dens utgjør fare for infrastruktur eller mannskap ombord. Videre regulerer ISPS-koden tiltak som gjelder ved de forskjellige sikkerhetsnivåene, hvor det ved nivå 1 skal gjennomsøkes/lyses, ved 2 skal det brukes røntgen og ved 3 en eventuell nekt av uledsaget bagasje. (Forordning 725/2004.)
Norge har som respons til angrepet på Nord Stream ledningene valgt å heve beredskapsnivået på en rekke norske havner til nivå 2. Dette medfører at alle skipene som skal ha anløp til disse havnene må være på beredskapsnivå 2.

Skip har i dag store mengder *nød og beredskapsutstyr,* som er påkrevd for at fartøyene skal være i drift.. Dette gjør det naturlig å kartlegge hvilket kritisk utstyr det må vernes om. Utstyret er en del av den viktige beredskapen i tilfelle en hendelse, og bør derfor vernes om, dette kan for eksempel være medisinsk utstyr som utgjør kritisk beredskap ombord.

Selv om ISPS-koden i stor grad handler om sikring mot terror og piratvirksomhet, altså begreper som faller under "security," dekker den også "safety." En sabotasje av eventuelt *nød- og beredskapsutstyr,* vil kunne hindre skipet i å seile, men ikke utøve noe direkte fare mot skipet initialt.

Besetningens størrelse vil i stor grad komplisere sikkerhetsarbeidet ombord. Større mannskap stiller større krav til en vurdering ettersom det er flere faktorer å ta hensyn til. Det vil være

flere *eksisterende sikkerhetsmessige oppgaver* som må vurderes, hvor det med økende mannskap vil være et mer komplekst sikkerhetsbilde. "*Opplæringskrav i rederiet,"* danner grunnlaget for dette og skal per lovverket kartlegges.

punkt 10 sier *"eksisterende sikkerhetsutstyr til beskyttelse av passasjerer og besetning"* Uttrykket sikkerhet er et begrep som i sin oversettelse kan miste sin hensikt. For å få korrekt tolking av ordlyden blir det derfor naturlig å se i den originale utgaven av ISPS-koden på engelsk. Her bruker ordlyden både "security" og "safety" der førstnevnte er relevant for vår problemstilling og omhandler sikring.

Under situasjoner hvor beste avgjørelse er å måtte evakuere skipet, stiller punkt 11 krav til at*"rømnings- og evakueringsveier og mønstringsstasjoner som skal opprettholdes for å sikre at evakuering av fartøyet foregår rolig og sikkert."* Opprettholdes disse, så skaper det en trygghet i evakueringsplanen.

Det er vanlig å bruke private leverandører av sikkerhet, et godt eksempel her kan være væpnede sikkerhetsvakter, som er mye brukt som et sikringsmiddel mot piratvirksomhet. *"gjeldende avtaler med private sikkerhetsselskaper som leverer sikkerhetstjenester på fartøyer og i havner, og"* Punkt 12 Pålegger CSOen å sette seg inn i hvilke slike avtaler som er aktive.

Det er jf. punkt 13 viktig at sikkerhetsoffiser ser over og innhenter informasjon om de *"gjeldende sikkerhetstiltak og -prosedyrer, herunder framgangsmåter ved inspeksjon og kontroll, identifikasjonssystemer, overvåkingsutstyr, besetningens identifikasjonsdokumenter og kommunikasjon, alarmer, belysning, adgangskontroll og andre hensiktsmessige systemer."* Dette er viktig slik at sikkerhetsoffiserer får kontroll over de diverse tiltakene og opplysningene som trengs, slik at det går an å ta en vurdering av fremgangsmåtene ved inspeksjon av diverse systemer og utstyr.

8.6 ADGANGSPUNKTER

I avsnitt 8.6 står det:

"En sårbarhetsvurdering av et fartøy skal undersøke hvert enkelt av de identifiserte adgangspunktene, herunder åpne dekk, og vurdere muligheten for at de kan brukes av enkeltpersoner som måtte ønske å bryte sikkerheten. Dette omfatter adgangspunkter som er tilgjengelige både for personer som har rettmessig adgang, og for personer som ønsker å oppnå ulovlig adgang"

1. I 8.6 er ordlyden presisert med å gå inn på at besetning av et fartøy skal undersøke skipets identifiserte adgangspunkter. Dette kan trekkes inn ved at blindpassasjerer prøver å snike seg om bord. Det finnes eksempler på saker hvor blindpassasjerer sniker seg om bord ved å klatre opp bak på roret mens skip ligger til kai. Som tidligere nevnt i oppgaven er det også saken med West Hercules hvor klimaaktivister i så måte kan sees på som blindpassasjerer der de klarte å snike seg om bord på plattformen. Dette kan også dras inn mot rutiner for vakthold og det at vakthold har utkikk for eventuelle blindpassasjerer. Disse utgjør som regel ikke noen fare, men dersom en blindpassasjer kommer seg ombord, kan vel også en sabotør/terrorist få det til?

8.7 SIKKERHET OM BORD

Vi tar for oss neste punkt i ISPS del B som er 8.7. Her beskrives ordlyden slik at tiltakene og retningslinjene skal tas stilling til at de skal være relevante. For å ta stilling til å se om disse er relevante, så kan vi sammenligne sikkerhetstiltakene og retningslinjene som er nåværende med nylige hendelser.

"En sårbarhetsvurdering av et fartøy skal ta stilling til om gjeldende sikkerhets tilknyttede tiltak, retningslinjer, rutiner og virksomhet fortsatt er relevante, både under normale forhold og i nødssituasjoner, og skal fastsette retningslinjer for sikkerheten som omfatter:"

.1 de adgangsbegrensede områdene,
.2 fremgangsmåtene ved brann eller i andre nødssituasjoner,
.3 nivået på overvåkningen av fartøyets besetning, passasjerer, besøkende, selgere, reparatører, havnearbeidere osv.,
.4 sikkerhets patruljens hyppighet og effektivitet,
.5 systemer for adgangskontroll, herunder identifikasjonssystemer,
.6 systemer og framgangsmåter for sikkerhets tilknyttet kommunikasjon,

.7 sikkerhetsdører, -sperringer og -belysning, og
.8 eventuelt sikkerhets- og overvåkingsutstyr og eventuelle sikkerhets- og overvåkingssystemer.

En hendelse vi kan ta for oss er kapringen av skipet Monjasa Reformer i Guyana bukta. Her var det en besetning på 16 personer som måtte gjemme seg i et safe room på grunn av kapringen av skipet. Sikkerhetstiltaket her er safe rommet, og i denne hendelsen ble døra til rommet besetningen gjemte seg i brutt opp. Altså sikkerhetstiltaket som ble laget for denne hendelsen, var ikke tilstrekkelig (Matthews, 2023).

Videre er det retningslinjer som f.eks. tilsier når det skal brukes og hvordan. Dette er et tiltak som skal beskytte besetningen, men i dette tilfellet ga ikke tiltaket tilfredsstillende resultat. Dette kan f.eks. ha med at retningslinjer ikke ble fulgt under hendelsen. Eller at retningslinjene ikke var relevante nok til denne situasjonen.

Ordlyden fortsetter ved å beskrive sikkerhetstiltak, og retningslinjer ved relevansen av dem både under normale forhold og i nødssituasjoner. For å forstå dette så tar vi det samme eksempelet vi brukte ovenfor med bruk av safe room. Denne hendelsen var en nødssituasjon der sikkerhetstiltaket var safe room. Selv om sikkerhetstiltaket i denne hendelsen ikke var tilstrekkelig nok, så er det fremdeles relevant med tanke på hvor livreddende et safe room kan være.
Tar vi for oss relevansen for slike tiltak med problemstillingen vår og skip i norske sektorer, så er risikoen for kapring ikke så veldig stor.

Siste del av ordlyden er at disse tiltak ikke bare er relevante, men også fastsetter disse retningslinjene sikkerheten som omfatter de punkter som står skrevet over. I den originale versjonen på sitt originalspråk står det “should”, noe som betyr bør, og ikke “skal” som det står i den norske versjonen.
Uansett, så beskriver ordlyden at vurderingen ovenfor sikkerhetstiltakene og rutinene skal skape retningslinjer for sikkerheten om bord.

Det er viktig å ha kontroll over hele skipet, og i henhold til ISPS del B 8.7, skal sårbarhetsvurdering ta stilling til det gjeldende sikkerhet rundt *adgangsbegrensede områder.*

Vi tar for oss et eksempel hvor bro er låst når skipet ligger til havn. Dette er et gjeldende sikkerhetstiltak som er i bruk under normale omstendigheter når skipet losser. Dette er et sikkerhetstiltak som er laget grunnet det ikke skulle være noen på bro uten offiser tilstede. Det er også mye kritisk utstyr på bro som ikke skal misbrukes.

Det blir så skrevet under 8.7 at *fremgangsmåtene under nødssituasjoner og normale forhold skal være relevante.* Ordlyden her bruker en presisjon på brann, så her kan vi ta for oss at det burde være jevnlige tester på situasjoner rundt brann. En nødssituasjon som er relevant i forhold til vår problemstilling er at det skjer sabotasje med sprengning eller at noe settes fyr på. Under normale forhold kan vi ta for oss en brannøvelse, hvor det skal terpes på de rutiner som er satt og at alle gjør det deres oppgave er.

Overvåkningen av mannskapet om bord skal også settes tiltak til og det skal finnes ut om dette er relevant nok. På bro så er det lydopptak av alt som blir sagt om en ulykke eller annen situasjon skulle oppstå. Med lydopptak vil etterforskere i etterkant av hendelsen kunne forstå hendelsesforløpet, og dette vil da kunne hjelpe forståelse for nye hendelser.
Når det kommer besøkende eller arbeidere som ikke er en del av besetningen, så skal det alltid være noen fra besetning med for å holde oppsyn. Dette er på grunn av at det er en ekstra sikkerhet å vite hva de evt gjør om bord og hvorfor.

For å forstå omfanget av det neste som kommer inn under 8.7, så må vi lese originalteksten av loven på grunn av tapet av forståelsen i oversetningen. Det står i originalteksten at det skal sjekkes om sikkerhets patruljen om bord har relevant nok erfaring til å kunne være effektiv i situasjoner. Sikkerhetspatruljen er den delen av besetningen som har roller som for eksempel røykdykkere. Dette er relevant fordi effektivitet er en viktig faktor i nødssituasjoner, men også generelt under helt normale omstendigheter.

Det er viktig med å vite hvem som har tilgang til diverse utstyr og områder om bord. Da er det som følger viktig med *systemer for adgangskontroll og det å ha identifikasjonssystemer.* Dette punktet står også i skipssikkerhetsloven §39, andre ledd. Vi kan ta for oss relevansen med slike systemer ved å kunne forsikre at de personer som kommer om bord, er den de har oppgitt. Det finnes personer som vil prøve på alt for å få det en vil ha, og da er det villig til å bruke annen identitet for å få det til. Derfor er det viktig å ha system for å kunne identifisere enhver som vil om bord i dette tilfellet. Det neste punktet i 8.7 beskriver kommunikasjonen

og om fremgangsmåtene for sikkerhets kommunikasjon fremdeles er relevant. Dette kan dras inn med å kunne kommunisere uten å oppgi sensitiv informasjon. Dette er også relevant med dagens situasjon hvor cyberangrep er høyst sannsynlig, og det er sjanse for at kommunikasjonsutstyr kan tjuvlyttes.

Det kan også tas i bruk sikkerhetstiltak som det å ha *sikkerhetsdører, sperringer og belysning* om bord. Her kan vi ta med neste mulige sikkerhetstiltak under dette som eventuelt beskriver det å ha med overvåkningsutstyr. Her kan vi ta med eksempel om at *belysning og overvåkning* er veldig relevant. Under operasjoner som tilsier at skipet ligger i ro så er det viktig å ha belysning slik at det er mulig å se for besetningen som jobber på dekk, og overvåkning slik at det er mulig å se arbeidet bli gjort.

8.8 BESETNINGENS SIKKERHET

Forrige punkt handlet om relevansen til eksisterende sikkerhetstiltak, mens 8.8 handler om hva eller hvem som er viktig å beskytte.

"En sårbarhetsvurdering av et fartøy skal ta stilling til hvilke personer, aktiviteter og tjenester og hvilken virksomhet som er viktig å beskytte. Disse omfatter:
.1 fartøyets besetning,
.2 passasjerer, besøkende, selgere, reparatører, havneanleggets personell osv.,
.3 evnen til å opprettholde sikker fart og kriseberedskap,
4. lasten, særlig farlig last og farlige stoffer,
.5 skipsforsyningene,
.6 fartøyets eventuelle sikkerhetskommunikasjonsutstyr og -systemer, og
.7 fartøyets eventuelle utstyr og systemer for overvåking og sikkerhet"

Dette punktet utdyper ISPS kodens del A punkt 8.4.2 som lyder "*identifisering og vurdering av vesentlige funksjoner om bord som det er viktig å beskytte"*. Der denne har et vesentlig stort omfang ved ordlyden funksjoner, presiserer 8.8 med personer, aktiviteter, tjenester og virksomhet. Identifisering og vurdering kan også i så måte bety å ta stilling til.

Det første punktet omhandler *fartøyets besetning* der mannskapet bord som det skal tas stilling til rundt viktigheten for beskyttelse. Besetningen vil alltid være en viktig faktor som trengs beskyttelse, foruten en besetning vil skipet ikke kunne driftes.
Det andre punktet *passasjerer, besøkende, selgere, reparatører, havneanleggets personell osv,* er menneskene rundt som besetningen vil komme til å håndtere. Selv om det sjeldent er passasjerer på tankskip vil det ofte være annet personell som kommer om bord ved for eksempel reparasjoner og vedlikehold.
Evnen til å opprettholde sikker fart og kriseberedskap, her ser vi en presisering av aktivitet som må beskyttes. Der opprettholdelse av sikker fart er forankret i loven, "Ethvert fartøy skal alltid gå med sikker fart" (sjøveisreglene, regel 6). Sikker fart vil være en betydelig viktig aktivitet som kan være sårbar. Der ved f.eks. i en situasjon som krever presis navigering og der små korreksjoner er viktige, kan en uventet økning av momentum utgjøre skade. Som tidligere nevnt er styringssystemet styrt av datamaskiner, om systemet var kompromittert i denne situasjonen kunne farten ha blitt kontrollert utenfra. Det er da viktig at det finnes tiltak til å beskytte sikker fart. Overvåkende navigatører kan være et tiltak. Kriseberedskap er også en aktivitet som er sårbar der om det først skjer en krise, vil kriseberedskapen være utrolig viktig for håndtering og ettermæle.
lasten, særlig farlig last og farlige stoffer. Last som i gods eller varer som fraktes, herunder til vår problemstilling olje eller gass. Der både olje og gass kan regnes som farlig last. Olje og gass kan regnes som farlig last med tanke på konsekvensene om påtenning skulle skje. Hvis vi ser for oss at en tankbåt som frakter olje holder på å losse, og det skjer en elektrisk feil i computeren som gjør at oljen blir antent. Dette kan ende opp i en eksplosjon hvor det blir fare for liv og andre verdier.

Skipsforsyningene. Skipets proviant, brensel osv. må ikke forveksles med tilbehør som er skipets løse gjenstander som brukes over lengre tid. Slik som f.eks. navigasjonsutstyr og redningsutstyr (Falkanger & Bull, 2010, s,28).

Fartøyets eventuelle sikkerhetskommunikasjonsutstyr og -systemer, på tankskip er dette sikkerhetskommunikasjonsutstyr og sikkerhetssystemer. Her kan vi ta for oss VHF(Very high frequency) som et sårbart element, hvor konsekvensen for at den slutter å virke kan være alvorlig. VHF brukes som et radiosystem hvor skip kan kommunisere med andre skip, flyttbare innretninger og landbaserte stasjoner osv. På VHF deles informasjon som er til nytte

for alle skip innenfor samme sektor. Dette er viktig for norske tankbåter der radiosystemet brukes til blant annet nødkommunikasjon.

Fartøyets eventuelle utstyr og systemer for overvåking og sikkerhet. Utstyr og systemer for overvåkning og sikkerhet kan i så måte være "ecdis"(Electronic Chart Display and Information System*)* eller radar. Der for eksempel radar brukes til å overvåke seilasen og for sikkerhet for sammenstøt. Det kan også nevnes at det er flere systemer på bro som brukes til overvåkning og sikkerhet, for eksempel ved ulykke der lydopptak blir lagret. I ordlyden brukes det fra forrige punkt bindeordet *og.* Der ordlyden bruker sikkerhetssystemer er det viktig å skille at forrige punkt presiserer kommunikasjon. Ecdis i så måte kan også sees på som kommunikasjonsutstyr, der informasjon mottas og sendes for å skape et bilde av posisjoner og informasjon fra AIS. Men hovedformålet med ecdis er til bruke overvåkning av seilas og andre skip.

8.9 OMFANGET AV EN SÅRBARHETSVURDERING

Videre skal vi se på 8.9 der dette punktet handler om mulige trusler.

En sårbarhetsvurdering av et fartøy skal ta stilling til alle mulige trusler, som kan omfatte følgende typer sikkerhetshendelser:

.1 skade på eller ødeleggelse av fartøyet eller et havneanlegg, f.eks. ved hjelp av sprengstoff, ildspåsettelse, sabotasje eller hærverk,
.2 kapring eller kidnapping av fartøyet eller av personer om bord på fartøyet,
.3 ulovlige inngrep i lasten, viktig utstyr eller viktige systemer på fartøyet eller skipsforsyningene,
.4 ulovlig adgang eller bruk, herunder forekomst av blindpassasjerer,
.5 smugling av våpen eller utstyr, herunder masseødeleggelsesvåpen,
.6 bruk av fartøyet til å transportere personer som har til hensikt å forårsake en sikkerhetshendelse, og/eller utstyret til disse personene,
.7 bruk av selve fartøyet som våpen eller som et middel til å forårsake skade eller ødeleggelse,
.8 angrep fra sjøsiden mens fartøyet ligger i havn eller for anker, og
.9 angrep mens fartøyet er til sjøs

Dette punktet presiserer en viktig del av sårbarhetsvurderingen, for det å ta stilling til alle mulige trusler er høyst viktig for å skape en god vurdering. Som de andre punktene under del B er dette en presisering av Del A, spesifikt 8.4.3. "*identifisering av mulige trusler mot vesentlige funksjoner om bord og sannsynligheten for at de skal oppstå, med det formål å fastsette og prioritere sikkerhetstiltakene".*

Det første punktet handler om *"Skade eller ødeleggelse på fartøyet"*, med eksempler for å klargjøre punktet. Eksemplene dekker et bredt spekter, noe ordlyden til første del også gjør. Der det viser til alt fra sprengstoff til hærverk. Noe av det første en tenker på ved terror er bruken av sprengstoff. Som nevnt innledningsvis ble USS Cole og M/V Limburg utsatt for terror ved bruk av sprengstoff. Dette kan også være en reell trussel i Norske farvann også, der tankbåter kan bli utsatt for målrettede detonasjoner. Vi har tidligere diskutert muligheten for at droner kan brukes som en "selvmordsbomber", noe som støtter dette.

"Kapring eller kidnapping av fartøyet eller av personer om bord på fartøyet" er neste element. I dag er kapring ofte noe som forbindes med piratvirksomhet, men det kan også brukes til f.eks. terror. Skipet kan da bli brukt som et medium for å utføre en terrorhandling eller en annen ulovlig handling. Det skal også nevnes at ved en kraftig eskalering fra klimaaktivister, kan skip bli kapret for å sende et budskap. Selv om dette er lite sannsynlig, er det verdt å ta til etterretning.
"ulovlige inngrep i lasten, viktig utstyr eller viktige systemer". Som tidligere diskutert er teknologi i stadig utvikling, dette skaper store utfordringer. Det å ta hensyn til trusler mot *inngrep i viktige systemer* er da særdeles viktig. I og med at dette er et omfattende element så vil vi særlig vise til 8.4 punkt 11 der det viser til *innhenting av sakkyndige nær det gjelder datasystemer.* Det bør også tas hensyn med tanke på lasten, der på tankbåter, dette er enten olje eller gass. Svært eksplosive stoffer. Ved strategisk plassering av eksplosivene vil effekten kunne bli mangedoblet. Da er det viktig at det også tas hensyn til "*ulovlig adgang eller bruk, herunder forekomst av blindpassasjerer,"* Der ut fra en god utredning av truslene fra dette, det lages gode tiltak for å hindre uvedkommende.

"*smugling av våpen eller utstyr, herunder masseødeleggelsesvåpen,"* Med dagens situasjon der Russland driver en offensiv i Ukraina, kan det tenkes at skip smugler våpen eller annet utstyr for Russland eller Ukraina. Den norske handelsflåten leverer olje og gass til baltiske

land, og da kan det tenkes at disse brukes som medium for å innføre ulovlig utstyr. Både Russland og Ukraina; pro-Ukrainske, har tilstedeværelse i Østersjøen. Et våpen kan også sees på som en person med spesialistferdigheter, f.eks. spesialist innen sprenging. 8.9 presisere at dette bør vurderes ved punkt 6, "*bruk av fartøyet til å transportere personer som har til hensikt å forårsake en sikkerhetshendelse, og/eller utstyret til disse personene,"*.
Som tidligere nevnt kan skip utnyttes som et medium til bruk av terror eller sabotasje. Dette belyser neste punkt; "*bruk av selve fartøyet som våpen eller som et middel til å forårsake skade eller ødeleggelse,"*. Der for eksempel et tankskip ligger tett opp mot en FPSO, flyterigg, og laster, for så å bli styrt rett inn i flyteriggen.'

"angrep fra sjøsiden mens fartøyet ligger i havn eller for anker" er ingen trolig trussel i Norge i dag, men som tidligere sagt ved en eskalering fra Russisk side er det vanskelig å vite. Det har vært tilfeller der det har blitt festet ting til skroget av et skip, se nyhetsartikkelen om fartøyet som ankom Kvinnherad med kokain i poser festet til skroget. (*Største Kokainbeslag Nokosinne På Vestlandet – NRK Vestland*, 2023). Dette er ikke akkurat et angrep, men det belyser sårbarheten et skip har ved havn eller for anker. Her ser vi for oss at dette kan ha blitt festet til skroget mens det lå til ankers eller i en havn. Dette kunne like gjerne vært eksplosiver med en detonator. Det samme kan skje ved *"angrep mens fartøyet er til sjøs",* men i store trekk er det nok tenkt på som typiske trekk fra pirater, der de seiler små båter opp mot skutesiden for så å klatre ombord. Det samme ved havn eller for anker.

En sårbarhetsvurdering skal gjøres for området en seiler i, men det er viktig å ha i tankene at det er flere nyanser som kan spille inn. Dermed er det viktig at en gjør en omfattende vurdering av trusler som kan forekomme som ISPS koden 8.9 presiserer. "Det er bedre å være føre var en etterpåklok". Og da må man ved sårbarhetsvurderingen ta hensyn til trusselbildet som bl.a. PST og NSM har gitt sine vurderinger av.

8.10 SÅRBARE OMRÅDER

En sårbarhetsvurdering inneholder et bredt spekter, og skal ta høyde for bredt spekter sårbarheter. Isps-kodens punkt 8.10 sier følgende:

"En sårbarhetsvurdering av et fartøy skal ta hensyn til alle tenkelige sårbare områder, som kan omfatte:"

Dette pålegger at alle sårbare områder på gitt fartøy skal tas i betraktning i sårbarhetsvurderingen. Videre viser punkt 8.10 til en rekke forhold som kan være aktuelle, uten at dette er pålagt. Dette tilsier at punktene må vurderes opp mot aktuelt fartøy og andre forhold som innvirker på fartøyets sårbarhet. de tenkelige sårbarhetene som gis er:

.1 "konflikter mellom forskjellige sikkerhetstiltak, "
.2 "konflikter mellom oppgaver om bord på fartøyet og sikkerhetsmessige oppgaver, "
.3 "vaktoppgaver, besetningens størrelse, særlig med hensyn til konsekvensene for besetningens tretthet, aktpågivenhet og ytelse, "
.4" eventuelle påviste mangler ved sikkerhetsopplæringen, og "
.5"eventuelt sikkerhetsutstyr og eventuelle sikkerhetssystemer, herunder kommunikasjonssystemer."

Her kan vi lese av ordlyden at sårbarhetsvurderingen skal ta hensyn til et bredt spekter av sårbare områder. 8.10 definerer videre eksempler på slike områder som er tenkelige scenarioer som skal tas høyde for i vurderingen.

Første punkt handler om:
"Konflikter mellom forskjellige sikkerhetstiltak," Konflikter kan sees på som motsetninger mellom forskjellige sikkerhetstiltak hvor for eksempel et sikkerhetstiltak vil kunne eliminere virkningen til et annet. Fra en fremmed aktørs synspunkt vil det kunne være interessant å kartlegge slike sikkerhetstiltak for å finne sikkerhetshull som kan utnyttes til deres formål. Dette kan gjøres ved å utløse bestemte sikkerhetshendelser for å provosere respons.

Videre viser punkt 2 til:
"Konflikter mellom oppgaver om bord på fartøyet og sikkerhetsmessige oppgaver"
Her legges fokuset på de forskjellige oppgavene ombord og hvordan disse løses. Fokuset faller her i større grad på den menneskelige faktoren, og hvordan de som har sitt arbeid om

bord samvirker. Det kan oppstå sikkerhetshull ved at oppgaver og da spesielt sikkerhetsmessige oppgaver motsetter hverandre.

Arbeid på skip er utmattende, hvor det trekkes tette bånd mellom nattarbeid, lite søvn og en svekking i oppmerksomhet, yteevne og risiko for å gjøre feil (Andersen Ellen Jul, August 2006.) Dette legger grunn for en sikkerhetsrisiko, noe som belyses i neste punkt i lovverket; *"Vaktoppgaver, besetningens størrelse, særlig med hensyn til konsekvensene for besetningens tretthet, aktpågivenhet og ytelse."*

"Eventuelle påviste mangler ved sikkerhetsopplæringen"
En essensiell del av sikkerheten om bord ligger i mannskapet. kvalitetssikring oppnås gjennom å detektere eventuelle feil og mangler. Ved å oppdage mangler ved sikkerhetsopplæringen om bord, vil man kunne finne feil som hindrer mannskapet i å avverge farlige situasjoner som ellers ville kunne unngås.

Dette videreføres også til utstyret og systemene, som skal hjelpe de som har sitt arbeid ombord i å gjennomføre sikkerhetspolitikken som føres av rederiet. *"Eventuelt sikkerhetsutstyr og eventuelle sikkerhetssystemer, herunder kommunikasjonssystemer."*
Den engelske utgivelsen av regelverket viser her til "Security," noe som viser til akutte *sikkerhetssystemer,* og spesifiserer videre at dette også gjelder *kommunikasjonssystemer.*

4.0 DISKUSJON

I de forrige kapitlene, gjør vi rede for hvilke lovbestemmelser som danner lovverket for en sårbarhetsanalyse, i lys av dette vil vi videre diskutere funnene rundt problemstillingen vår:

> *Hva ligger i skipssikkerhetsforskriftens (og ISPS-kodens) krav om at det må gjøres en sårbarhetsvurdering for skip – særlig med tanke på tankbåter i norske farvann i lys av dagens utfordrende sikkerhetspolitiske situasjon?*

Vi vil se på hendelser som vi mener er aktuelle i norske farvann i dag, og bruke regelverket for å belyse disse. Videre vil vi diskutere aksjoner vi mener kan utgjøre et risikomoment i norske farvann, og vise til hvorvidt regelverket dekker dette.

Som nevnt, kommer ISPS-koden som et direkte svar til terrorhandlingene 9/11, hvor fly kapres og flys inn i bygninger. Det er her tenkbart at denne terroraksjonen er overførbar til det maritime, men hvordan?

Etter at krigen i Ukraina brøt ut, og EU ikke lenger importerer olje og gass Russland, er nå Norge en kritisk leverandør til Europa. Dette gjør tankbåter som henter og leverer disse varene til utsatte mål ved en eventuell eskalering i konflikten. Det å kapre en tankbåt, er absolutt mulig. Kapring av skip er noe vi jevnlig ser i blant annet Afrika hvor dette gjøres for økonomisk vinning. Dersom man skal overføre problemstillingen til norske farvann, er ikke kapring for økonomisk vinning like aktuelt, men man kan derimot tenke seg at tankbåter kan bli brukt i terror/sabotasjeaksjoner. Det kan tenkes at en gass/oljetanker for eksempel seiles inn i havnen til en storby for å der enten eksploderes eller, hvor det trues med sprenging grunnet et eller annet motiv. Det potensielle skadeomfanget fra en gass/oljetanker er naturlig veldig stort, og vil kunne utgjøre stor skade dersom lasten skulle antennes.

Hvis vi ser på ISPS-kodens paragraf 8-9, sier den følgende:

> *En sårbarhetsvurdering av et fartøy skal ta stilling til alle mulige trusler, som kan omfatte følgende typer sikkerhetshendelser:*
> *.2 kapring eller kidnapping av fartøyet eller av personer om bord på fartøyet,*
> *.7 bruk av selve fartøyet som våpen eller som et middel til å forårsake skade eller ødeleggelse,*

Dette viser til relevansen i ISPS-kodens del B. Punktene over har direkte sammenheng med kapring og bruk av fartøy som våpen, men for å komme til punktet der man har kontroll på et fartøy i den forstand, er det mange barrierer man må komme seg forbi. Lovverket har en stor bredde og dekker egentlig alle tilfeller hvor fartøy kan brukes som *våpen* eller middel til å *forårsake skade eller ødeleggelse.* Derav må en sårbarhetsvurdering ta stilling til en stor mengde mulige hendelser.

Om en skulle ønske å ta seg ombord på et skip med ønske om å utrette skade ville første steg er gjerne å bryte sikkerheten for å komme seg ombord. Punkt 8.6 er et helt eget punkt dedikert til skipets adgangspunkter og omhandler sikkerheten rundt de adgangspunktene som

benyttes av de som har lovlig tilgang til fartøyet. for å få tilgang kan brudd på tiltak som gis av 8.6 være kritiske. Dette kan være ting som: *overvåking, systemer for adgangskontroll, sikkerhetsdører/sperringer og sikkerhetspatruljer.* Å komme seg ombord på skip er en problematikk som stadig dukker opp. Som nevnt i tidligere eksempler har personer klatret opp ankerkjettinger, opp på ror, sneket seg ombord mm. Dette utgjør derfor et viktig punkt for fartøyets sikkerhet. Et annet adgangspunkt er via last. Lovverkets punkt 8.9 punkt 3 gir at følgende faren for:

"ulovlige inngrep i lasten, viktig utstyr eller viktige systemer på fartøyet eller skipsforsyningene"

Skal tas med i en vurdering. Det kan være smugling av våpen, person mv. som smugles ombord med formål om å ta kontroll over fartøyet. Derfor utgjør også kontrollen på alt som tas ombord et viktig moment.

Når uønskede personer først har fått tilgang til skipet med ønske om å utøve terror, kan neste mål være å få kontroll over kritisk infrastruktur ombord. Dette kan gjerne være broen og maskinrom for å kunne styre fartøyet uavbrutt. 8.7 Definerer da videre at en sårbarhetsvurdering tar stilling til de gjeldende sikkerhetstiltakene og fastsette retningslinjer for sikkerheten. Første punkt under 8.7 pålegger en slik vurdering av *de adgangsbegrensede* områdene, som vil være områder kritisk for skipets drift.

Videre så er det også et annet tenkelig scenario i norsk farvann: cyberangrep. Dette er et scenario som nå i nyere tid har blitt svært aktuelt, hvor det å ha informasjon kan bli brukt som våpen. Tiltak som kan tas i bruk for å forbedre sikkerheten mot eventuelle cyberangrep er å drive opplæring internt. I ISPS del B 8.10 så står det et punkt: dette med å finne *eventuelle påviste mangler ved sikkerhetsopplæringen.* Dette hjelper med å styrke opplæringen blant besetningen, og det vil da videre kunne styrke oppmerksomheten. Man vil også da kunne ta utgangspunkt i å få lære opp det som mangler. På denne måten vil det videre kunne dannes en kombinasjon mellom et bra system og god oppmerksomhet fra besetning. Videre vil det si bedre sjanse om å stoppe cyberangrep

I ISPS del B punkt 8.3 står det slik at en sårbarhetsvurdering skal ta for seg: *radio- og telekommunikasjonssystemer, herunder datasystemer og nettverk*. Dette er viktig å ta for seg

med tanke på at cyberangrep kommer inn under disse systemene. Siden skip har blitt mer og mer avansert opp igjennom årene, så har også interessen for å kunne overstyre skip blitt høyere. Vi har nå kommet til en tid hvor nettverket og de andre systemene drives via teknologi. I sammenheng så er det også utviklet mye teknologi som har muligheter for å hacke seg inn på slike systemer. I tillegg da når skip er så verdifulle som de er, så er det også en større sannsynlighet for at slikt skjer.

Sårbarhetsvurdering i dette aktuelle scenarioet skal også ta for seg det som ISPS del B punkt 8.8 nevner: *fartøyets eventuelle sikkerhetskommunikasjonsutstyr og -systemer,* Denne går i mye av det samme som forrige punkt, men denne går mer inn på fokus rundt besetningens sikkerhet. Ordlyden gjennom 8.8 er at selve sårbarhetsvurderingen skal ta stilling til hva og hvem om bord på fartøyet som er viktig å beskytte.

Det som må tas stilling til i en sårbarhetsvurdering i tillegg til systemene som er blitt skrevet over. Det er dette med å finne *eventuelle påviste mangler ved sikkerhetsopplæringen,* og ta utgangspunkt i å få lære opp det som mangler. På denne måten vil det kunne dannes en kombinasjon mellom et bra system og god oppmerksomhet fra besetning. Videre vil det si bedre sjanse for å stoppe cyberangrep.

5.0 KONKLUSJON

Skipssikkerhetsforskriftens (og ISPS-kodens) krav om at det må gjøres en sårbarhetsvurdering for skip er som vi har vist meget omfattende. I dagens trusselbilde fremstår det som viktig at også tankbåter i norske farvann tar dette på alvor og gjør en grundig sårbarhetsvurdering i tråd med regelverket. Det skal også sies at informasjon som kan være viktig for en sårbarhetsvurdering ikke alltid er tilgjengelig.

Det er selvfølgelig alltid muligheter for å forbedre lovverket. Slik som situasjonen er i dag med nye utfordringer i norske farvann, kan det være bruk for et utdypende regelverk med tanke på nettverk og datasikkerhet. Dette er et stadig utviklende emne, med store teknologiske fremskritt. ISPS koden dekker dette, men det burde kanskje tillegges noen presiseringer? Ved tolkning av ISPS koden er det også viktig å ta original versjon til

etterretning, der den norske oversettelsen ikke alltid strekker til. Et godt eksempel på dette er at det ikke skjelnes mellom "security" og “safety” i oversettelsen. For en presisering i teksten kunne vi ha tenkt oss at ISPS koden brukte ordet “sikring” for sikkerhet, slik som Simonsen nevner i sin bok (Simonsen, 2022).

Sikkerhetsforskriften pålegger det norske lovverket å følge del A fra ISPS koden, men også store deler av del B. Det er ikke krav fra EU at Norge skal lovfeste deler av del B, men Norge har da valgt å ta det med. Vi ser da at elementene som er i del B er til stor nytte for sårbarhetsvurderingen. Der disse presiserer del A med både eksempler og elementer som skal tas hensyn til.

Nå i nyere tid med krigen mellom Ukraina og Russland, har også Norge blitt en av de større gassleverandørene til Europa, så da er det på tide at sårbarhetsvurderingene oppdateres.

6.0 KILDELISTE

Andersen, E. J. (2006, august 24). Helseeffekter av lange arbeidsskift og nattarbeid. Retrieved April 27, 2023, from https://tidsskriftet.no/2006/08/aktuelt-i-foreningen/helseeffekter-av-lange-arbeidsskift-og-nattarbeid

BBC NEWS | Middle East | Yemen ship attack 'was terrorism'. (2002, October 13). Retrieved May 2, 2023, from http://news.bbc.co.uk/2/hi/middle_east/2324431.stm

Bull, H. J., & Pettersen, T. H. (2010). *Skipssikkerhetsloven: med kommentarer*. Fagbokforlaget.

Dale, C. (2020 April 6) Hva er Red Team, og hvordan fungerer det? Retrieved May 2, 2023, from https://www.netsecurity.no/fagblogg/hva-er-red-team-og-hvordan-fungerer-det

EØS Forordning (2004) EUROPAPARLAMENTS- OG RÅDSFORORDNING (EF) nr. 725/2004 Retrieved May 2, 2023 from https://lovdata.no/static/NLX3/32004r0725.pdf

Falkanger, T., & Bull, H. J. (2010). *Sjørett*. Sjørettsfondet.

Fokus 2023. (n.d.). Etterretningstjenesten. Retrieved May 2, 2023, from https://www.etterretningstjenesten.no/publikasjoner/fokus/innhold

Høyland, H. Nordmann K. S (2022, 22 september) Uidentifiserte droner i Nordsjøen: vær på vakt. NRK. https://www.nrk.no/rogaland/uidentifiserte-droner-i-nordsjoen_-_-vaer-pa-vakt-1.16113256

IMO (2023) IMO, Retrieved May 2, 2023, from https://www.imo.org/

Kopperud, K.A., & Askildt, M. (2003). *Security at sea* (1st ed.). Norwegian shipping security.

Konsolidert forordning (EF) nr. (725.2004) Retrieved May 2, 2023, from https://lovdata.no/static/SF/32004r0725k-01.pdf

Kraftig økning av GPS-jamming over Finnmark – NRK Troms og Finnmark. (2023, February 24). NRK. Retrieved May 2, 2023, from https://www.nrk.no/tromsogfinnmark/kraftig-okning-av-gps-jamming-over-finnmark-1.16309499

Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven). (n.d.). Lovdata. Retrieved May 2, 2023, from https://lovdata.no/dokument/LTI/lov/1998-03-20-10

Matthews, C. (2023, March 29). Crew of tanker attacked by pirates barricaded themselves in safe room. Retrieved May 2, 2023, https://www.dailymail.co.uk/news/article-11918001/Crew-Danish-oil-tanker-attacked-pirates-barricaded-ships-safe-room.html

NAOB. (n.d.). *klimaaktivist - Det Norske Akademis ordbok*. NAOB. Retrieved May 2, 2023, from https://naob.no/ordbok/klimaaktivist

Nasjonal sikkerhetsmyndighet. (2023). Risiko 2023. Retrieved April 27, 2023, from https://nsm.no/getfile.php/1312547-1676548301/NSM/Filer/Dokumenter/Rapporter/Risiko%202023%20-%20Nasjonal%20sikkerhetsmyndighet.pdf?fbclid=IwAR1ry7WLumu0Jgw3sPNm-rRZm8k_hg-9F5jp-tTBMhK7TaZ_9GzjW3j0VoE

NOU Norges offentlige utredninger 2005: 14 - På rett kjøl. (n.d.). Regjeringen.no. Retrieved April 28, 2023, from https://www.regjeringen.no/contentassets/8f863e1a5d7b48739df2408827057485/no/pdfs/nou200520050014000dddpdfs.pdf

Ot.prp. nr. 87 (2005-2006) Om lov om skipssikkerhet (Skipssikkerhetsloven) Retrieved 2 May, 2023 from https://www.regjeringen.no/no/dokumenter/otprp-nr-87-2005-2006-/id189725/?ch=8

PST. (2023). Nasjonal trusselvurdering 2023. Retrieved May 2, 2023, from https://www.pst.no/alle-artikler/trusselvurderinger/ntv-2023/

Sabotasje mot hvalskute i Svolvær – NRK Norge – Oversikt over nyheter fra ulike deler av landet. (2010, April 3). Retrieved May 2, 2023, from https://www.nrk.no/norge/sabotasje-mot-hvalskute-i-svolvaer-1.7065231

Sikkerhetsforskriften. (2004) Forskrift om sikkerhet, pirat- og terrorberedskapstiltak og bruk av maktmidler om bord på skip og flyttbare boreinnretninger (FOR-2004-06-22-972). Lovdata https://lovdata.no/dokument/SF/forskrift/2004-06-22-972/KAPITTEL_2#KAPITTEL_2

Simonsen, S. (2022). *Skipssikkerhetsrett: det rettslige rammeverket for maritime operasjoner* (1st ed., Vol. 1). Fagbokforlaget.

Største kokainbeslag nokosinne på Vestlandet – NRK Vestland. (2023, April 18). Retrieved May 2, 2023, from https://www.nrk.no/vestland/storste-kokainbeslag-nokosinne-pa-vestlandet-1.16377742

Trusselvurdering 2018. (2018, January 30). PST. Retrieved May 2, 2023, from https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2018/

USS Cole Bombing — FBI. (n.d.). FBI. Retrieved May 2, 2023, from https://www.fbi.gov/history/famous-cases/uss-cole-bombing

Vissgren, J., Tomassen, J. H., & Nordvåg, H. B. (2019, april 29). Miljøaktivister klatret ombord på oljerigg. *NRK*. Retrieved May 2, 2023, from https://www.nrk.no/tromsogfinnmark/miljoaktivister-klatret-om-bord-pa-oljerigg-1.14453135