MASTEROPPGAVE

Emnekode: LED5009

Navn: Ole Andreas Lereim

International Maritime Organization's (IMO) guidelines on maritime cyber risk management - Innføring av cybersikkerhetskrav i norsk maritim bransje.

Dato: 24.05.2023

Totalt antall sider: 58

NORD universitet

www.nord.no

Innholdsfortegnelse

Forord

Denne masteroppgaven er utarbeidet studieåret 2022/23 ved masterprogrammet innen sikkerhet og kriseledelse ved Handelshøyskolen ved Nord Universitet. Oppgaven er en 30 studiepoengs faglig forskningsoppgave av et valgt emne, skrevet av Ole Andreas Lereim.

Jeg er utdannet IKT-ingeniør, og har jobbet hele mitt liv i Forsvaret. I perioden 2015 til 2022 jobbet jeg i Kystvakten, og ble meget fasinert av avdelingens oppdrag og mandat. I 2021 ratifiserte Norge FNs krav til cybersikkerhet til sjøs. Denne resolusjonen ble ført i pennen av FNs maritime organisasjon International Maritime Organization (IMO), og resolusjonen fikk navnet MSC.428(98)(IMO, 2017). Som ingeniør og offiser har maritim cybersikkerhet fasinert meg. Både fordi jeg opplever det som et teknisk krevende fagfelt men også fordi Norge er en stor sjøfartsnasjon med betydelige maritime interesser.

Norsk digital sikkerhet har vært et aktuelt tema siden Lysneutvalgets rapport i 2015 (Lysne, 2015), og har jevnlig vært et tema i nasjonale politiske debatter. I forskningsprosessen har jeg fått innblikk i hvordan den nasjonale strategien for digital sikkerhet materialiserer seg i den maritime sektoren, samt en forståelse for hvilke drivkrefter som får maritim digital sikkerhet på agendaen både i næringen og i sektoren som helhet. Selv om jeg ved oppgavens start hadde en forståelse for både maritim næring og digital sikkerhet, så har sammenstillingen av de to fagområdene vært svært spennende, lærerikt og gitt meg en forståelse og erfaringer som jeg vil ta med meg inn i fremtiden.

Det rettes derfor en stor takk til min veileder professor Mass Soldal Lund, som har bidratt med meget god veiledning. Takk for gode faglige innspill, tilgjengelighet og konstruktive tilbakemeldinger.

Sammendrag

Hvordan implementerer Norge og Sjøfartsdirektoratet en FN-resolusjon innen digital sikkerhet i maritim sektor? Hva er veien videre for å skape digitalt robusthet og resilliense i næringen? Den digitale sikkerheten settes på agendaen av Sjøfartdirektoratet på vegne av de politiske prioriteringene som til enhver tid er rådende. I forskningsoppgaven har fokus vært å kartlegge erfaringene som finnes både innen regulering og tilsynsmyndigheter, samt ved den utførende delen av næringen. Grensene mellom rollene er overlappende, den kjennetegnes som meget selvdrevet og tar i stor grad tak i utfordringer før det blir kravstilt fra staten.

Forskningsdesignet mitt har vært utforskende, med deskriptiv metode. Denne åpne tilnærmingen til oppgaven gjør at dataene har drevet fokuset og analysen av studien, samtidig som jeg prøver å sette mine funn inn i eksisterende teori for å kunne besvare min problemstilling:

Hvilken endringsreise skaper innføring av IMO MSC.428(98) (IMO, 2017) innen norsk maritim næring, og hvilke erfaringer knyttes til den?

Mine forskningsspørsmål har vært:

Hvor viktig er cybersikkerhet for maritim næring?

Hvilke aktører skal drive frem innføringen av IMO MSC.428(98) (IMO, 2017) i norsk sjøfart?

Hvilke erfaringer har næringen gjort seg i forhold til organisering og kompetanse for å løse kravene i IMO MSC.428(98) (IMO, 2017) på en mest effektiv måte?

Forskningen min indikerer at norske myndigheter har iverksatt en målrettet implementeringskampanje vedrørende IMOs cybersikkerhetsresolusjon mot den maritime næringen. Næringen har respondert på myndighetskravene, og er godt i gang med omstillingen. Myndighetene har i mindre grad fokusert på eget oppdrag om å tilrettelegge for kompetansebygging innen maritim cybersikkerhet og etablering av sektorielle støtteressurser for cybersikkerhet innen sektoren.

Endringsreisen innen maritim cybersikkerhet har nådd en milepæl, men den er ikke over. Det private næringslivet er mer omstillingsdyktig, enn myndighetene. Innføring av IMOs cybersikkerhetskrav framstod for de fleste i starten som en stor aktivitet, men etter hvert som kunnskapen om maritim cybersikkerhet øker blant de berørte partene. Så blir IMOs cyberkrav en delaktivitet, innen endringsreisen som er maritim cybersikkerhet. En reise som krever mer styring fra myndighetene, og en tematisert ledelse av innsats på tvers av departementer og etater for å understøtte næringens behov.

Summary

How does Norway and the Norwegian Maritime Directorate implement the UN resolution concerning cybersecurity in the maritime industry? What is the road ahead to build a robust and resilient digital foundation for the maritime industry. Nowadays, cybersecurity has earned its place at the table of the Norwegian Maritime Directorate due to the political priorities.

In this research paper the focus has been on surveying the experiences among regulatory- and supervisional authorities, and the executing part of the maritime branch. The borders that separates the roles are overlapping, but the Norwegian maritime industry is known to be highly adaptable to changing conditions. Characterized as a self-driven industry that quickly adopts to changes in the maritime market, without governmental guidance.

The research design has been exploratory, with an exploratory method. This open approach to the research paper has driven the focus and analysis of the study, simultaneously as I have put my findings in the contents of existing theories in order to answer my main science issue:

What is change does the introduction of the IMO MSC.428(98) (IMO, 2017) entail for the Norwegian maritime industry, and what are experiences that is associated with it?

My research questions have been:

How important is cybersecurity to the maritime industry?

Who are the main stakeholders who are to drive the implementation of IMO MSC.428(98) (IMO, 2017) in the maritime industry?

What experiences has the industry made when it comes to organizing and competence in order to comform the demands in IMO MSC.428(98) (IMO, 2017) in an effective way?

My reseach indicates that the Norwegian authorities has launched a purposeful campaign for an effective implementation of IMOs cybersecurity resolution for the maritime industry. The industry has responded in accordance with the authorities demands, and the changes of resolution is well under way. The authorities main focus has been on helping the maritime industry to cope with the demands, with a lesser focus on their own tasks connected to

including cybersecurity in the maritime education and the establishment of governmental computer emergency response teams to support the maritime industry.

The change journey associated with maritime cybersecurity has reached a milestone, but not the its end. The maritime industry is highly adoptable, in some instances better then the authorities. The introduction of IMOs cybersecurity requirements looked like a big activity, and while the knowledge of maritime cybersecurity grew the IMOs resolution grew in to a subtask. This journey need the authorities to map out the course, with a solid cooperation between the different governmental departments who controls the maritime industry.

1 Introduksjon

1.1 Overordnet perspektiv

I 1959 opprettet de Forente Nasjoner (FN) den internasjonale sjøfartsorganisasjonen (IMO)(Nations, 2021) for å samle, regulere og standardisere den internasjonale skipsfarten. Organisasjonen ble avtalefestet ti år tidligere i etterkrigstiden, der økt samhandling på tvers av landegrenser utviklet seg. IMOs oppgave er å fremme samarbeid mellom verdens styresmakter for å gjøre sjøfart så trygt som mulig, og forhindre forurensing fra skip(Nations, 2021). Eksempel på en konvensjon som IMO har iverksatt er STCW konvensjonen (The International Convention on Standards of Training, Certification and Watchkeeping for Seafarers)(SDIR, 1978), en internasjonal konvensjon som setter kvalifiseringskrav for skipsførere, offiserer og annet vaktgående personell på handelsfartøy.

I 2021 iverksatt IMO konvensjonen som regulerer cyberrisiko til havs, parallelt med at FN vedtok IMO Resolution MSC.428(98)(IMO, 2017). Denne resolusjonen stiller krav til rederier og andre skipseiere om hvordan cyberrisiko skal forebygges, og hendelser håndteres. Dette var den første reguleringen av maritim cyberrisiko som stiller felles krav til sjøfart. Før konvensjonen har de ulike nasjonene og virksomhetene brukt egne metoder og standarder av ulik kvalitet og effektivitet.

En resolusjon fra IMO er en anbefaling for medlemslandene, og ikke en utfyllende kravliste. Selv om skipssikkerhet og cyberhendelser innebærer store konsekvenser og enorme inntektstap for virksomhetene (Ritchie, 2019), står nasjonene ganske fritt til å tolke og etterleve standardene.

Sjøfartsdirektoratet har begrenset hvem som omfattes av reguleringen fra IMOs cybersikkerhetsresolusjon i Norge til å være fartøy av typen (SDIR, 2014):

- Lasteskip med bruttotonnasje på 500 eller mer
- Fiskefartøy med bruttotonnasje på 500 eller mer
- Flyttbare innretninger
- Passasjerskip sertifisert for mer enn 12 passasjerer i utenriksfart
- Passasjerskip sertifisert for mer enn 100 passasjerer i innenriksfart

- Passasjerskip som bruker drivstoff med flammepunkt under 60 grader, sertifisert for mer enn 12 passasjerer.

Når det gjelder organisasjoner, enten de er eksistensielt nødvendige eller økonomisk motivert, har det siste århundret vist en, på grensen til ekstrem nødvendighet for å ha evnen til å forandre og utvikle seg (Kotter, 2012). En større globalisering, økt digital sammenknytning og nye teknologier tvinger organisasjoner til å endre seg for å opprettholde produktivitet. Parallelt med denne utviklingen av en moderne organisasjon, øker sårbarheten for å bli utsatt for vinningskriminalitet fra kriminelle aktører. Oppgaven vil derfor ta utgangspunkt i Kotters åtte stegs teori om organisasjonsendring (Kotter, 1995), og sammenligne sentrale karakteristikker og prinsipper opp mål og hensikt med IMO Resolution MSC.428(98)(IMO, 2017).

Jeg ser på temaet maritim cybersikkerhet i konteksten av IMO resolusjon MSC.428(98). Norge har allerede ratifisert denne konvensjonen, og jeg ønsker å forske på hvordan konvensjonen vil gi en økt sikkerhetsmessig gevinst for norsk sjøfart.

En endringsprosess kan være krevende for en organisasjon. Innføringen av IMO Resolution MSC.428(98) (IMO, 2017) er i noen grad allerede iverksatt av innad i den norske maritime næringen, mens andre deler av næringen ikke ennå har startet på sin endringsreise. Det finnes noen erfaringer i bransjen da kravet ble implementert i 2021, og samdriftsorganisasjoner er blitt etablert. Men dog er implementeringen i startfasen, og implementeringsløpene er i stor grad i en tidlig fase.

Hensikten med denne studien er derfor å undersøke hvordan norsk maritim næring har operasjonalisert IMO Resolution MSC.428(98)(IMO, 2017), og om dette gir et adekvat digitalt grunnmur mot uønskede hendelser. Som et resultat av min forskning så håper jeg å kunne oppsummere mine funn som et veikart for denne endringsreisen med Kotter som et teoretisk fundament.

1.2 Problemformulering

Hvilken endringsreise skaper innføring av IMO MSC.428(98) innen norsk maritim næring, og hvilke erfaringer knyttes til den?

Mine forskningsspørsmål vi være:

Hvor viktig er cybersikkerhet for maritim næring?

Hvilke aktører skal drive frem gjennomføringen av IMO MSC.428(98) i norsk sjøfart?

Hvilke erfaringer har næringen gjort seg i forhold til organisering og kompetanse for løse kravene i IMO MSC.428(98) på en mest effektiv måte?

1.4 Avgrensinger av oppgaven

Forskningen avgrenses til å analysere funn i konteksten av Kotters åtte steg for endring (Kotter, 1995), herunder fokusere på trinnene fem til og med åtte. Det er i disse trinnene det settes fart og retning på endringsreisen, og jeg forventer å kunne anvende de data som mine forskningsspørsmål vil gi meg knyttet til begrepsavklaring, aktørkjennskap og erfaringer knyttet til IMO konvensjonen. Kotter legger vekt på at i denne fasen fjernes hindringer, enkle gevinster hentes hjem og nye endringer skapes og permanente løsninger forankres i virksomheten.

I og med at Norge allerede har ratifisert IMO Resolution MSC.428(98)(IMO, 2017) er fart og kurs for endringsreisen implementeringsstrategi allerede iverksatt.

De siste to trinnene i Kotters modell er endring av systemer som ikke er synkronisert med endringene, og skape en mer permanent forankring i organisasjonen. Disse trinnene gir en indikator på hvordan endingsreisen vil utvikle seg i et lengre perspektiv, og vil belyse faktorer for fremtiden som må utledes nærmere gjennom blant annet politiske beslutninger og videre forskning.

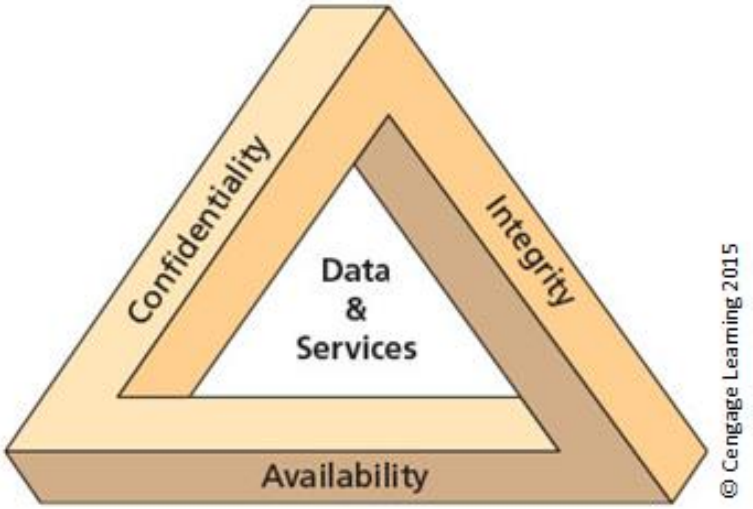
2 Bakgrunn

Formålet med litteraturkapittelet er å danne en forståelse for hva vi allerede vet om annen forskning og publikasjoner som kan være med på å kaste lys over problemstillingen. Her introduseres cybersikkerhet generelt og IMOs cybersikkerhetsstandard spesielt for å beskrive rammene for forskningen. I forskningen prøver jeg å sette innføringen av denne resolusjonen i et organisasjonsutviklende perspektiv, og jeg vil derfor også gi en kort innføring i Kotters åtte trinnsmodell for organisasjonstransformasjon.

2.1 Cybersikkerhet

Maritim næring er en av Norges eldste næringsaktiviteter. I dag jobber om lag 90 000 personer i næringa og det skapes verdier for til sammen 140 mrd. Inkluderes olje- og gassproduksjon, samt sjømatnæringen i definisjonen av den norske maritime næringen, så sysselsetter de i dag rundt 200 000(SDIR, 2020). Norge som nasjon har alltid vært en stor internasjonal maritim aktør, og Regjeringen satser på hav og at Norge skal ha en lederrolle i en global kontekst. Om lag trefjerde deler av all godstransport inn og ut av Norge skjer på kjøl.

Cybersikkerhet oppsummeres på et grunnleggende nivå som CIA-triaden (Mattord, 2020) som figur 1 viser . Hver enkelt side i triaden beskriver en dimensjon som informasjonen må inneha for å ivareta dens sikkerhet til informasjonen. Som de fleste trekantbaserte modeller, prøver man å ha en balanse mellom de tre punktene for å ivareta alle aspekter av informasjonssikkerhet. En ubalanse vil medføre mindre sikkerhet i triaden, og den ubalanserte delen vil være en eksponert angrepsflate for et digitalt angrep.



Figur 1: CIA modellen fra Cengage Learning 2015(Mattord, 2020)

Bokstaven C i modellen star for Confidentiality eller på norsk konfidensialitet. Med det mener vi at informasjonen er beskyttet på en måte som forhindrer uautoriserte mennesker eller systemer tilgang av våre data.

Bokstaven I står for Integrity, og oversatt til norsk så blir det integriteten til dataene. I det begrepet tillegger vi betydningen at dataene er riktige, komplett og at det ikke er blitt påvirket eller utsatt for uautorisert endring.

Bokstaven A står for Availability, som på norsk betyr at dataene er tilgjengelig for brukeren. Informasjonen skal være tilgjengelig for en godkjent bruker når vedkommende trenger det, og i rett format.

CIA triaden er grunnlaget for all IKT sikkerhet. Når man designer et sikkerhetssystem for en tjeneste eller teknologi prøver man å finne det optimale punktet mellom de tre entitetene i trekanten. Det vil si at om du endrer balansen mellom for eksempel konfidensialitet, så går det ut over tilgjengeligheten brukeren har til sine data.

CIA-triaden brukes primært om informasjonssikkerhet, mens cybersikkerhet defineres som systemer og infrastruktur som får IT-systemene til å virke sammen (Solms, 2013). von Solms

defensjon trekker frem at det er større sammen spill mellom informasjonssikkerhet og cybersikkerhet, og at det er en sameksistens mellom de for å ivareta sikkerheten til systemene.

I en maritim kontekst så omtales fartøyets datasystemer som enten et IT (Cisco, 2022) (standard IT system) eller OT (Cisco, 2022)(operasjons og kontrollsystem). Et IT-system vil være mer oppdatert og teknologisk modent da det benyttes primært hyllevare. Et angrep på et IT-system vil begrense seg til forretnings og organisasjonsdrift, men ikke kunne komme i inngripen med kritiske navigasjons og fremdriftssystemer. OT-systemet er som oftest tatt ombord i fartøyet som en del av byggeprosessen eller en større modernisering. Systemet er ikke knyttet sammen med IT-systemet, og er på den måten adskilt fra andre cyber sårbarheter. Blir et OT-system utsatt for et vellykket cyberangrep vil konsekvensene for fartøyets navigasjon og fremdriftssystemer være kritisk.

I Det Norske Veritas (DNV) sin Risiko og sårbarhets (ROS) analyse (DNV-GL, 2020) beskrives næringen som tett integrert i verdiskapningen i Norge og internasjonalt. Det trekkes frem at IT systemer (Vold, 2023))som benyttes i næringen er primært basert på hyllevare teknologi. Sårbarheten er først og fremst knyttet til skadevare rettet mot de mest brukte standardsystemer. IT-systemene er sårbare for eksterne angrep, men de styrer ingen fartøykritiske prosesser. DNV vurderte det som ikke nødvendig å utvikle egne IT-industrispesifikke retningslinjer for fartøy eller landkontor. I Norma Cybers årsrapport for 2023 (Vold, 2023) trekkes det frem at det primært er IT-systemer som angripes i cyberangrep, men at dette kan endre seg i fremtiden. DNV vurderer derfor at «det er lite behov for industrispesifikke retningslinjer for IT-systemene om bord og på kontoret».

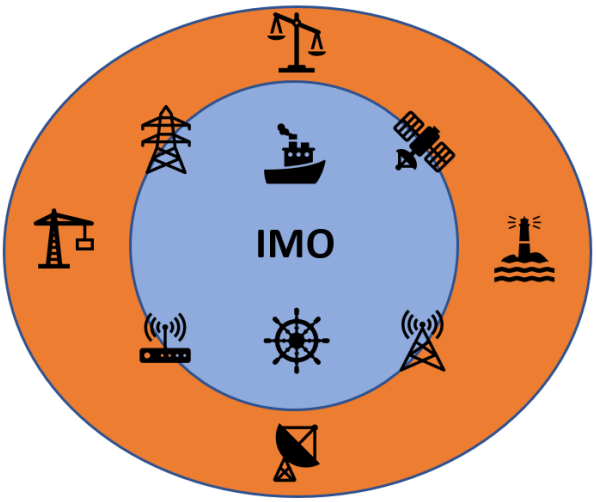
I DNVs ROS (DNV-GL, 2020) analyse trekker de frem at OT-systemene har tradisjonelt vært basert på proprietære teknologier, men nå brukes systemene mer og mer hyllevare-teknologi. Denne eksponeringen øker derfor systemenes sårbarhet for skadevare som er rettet mot standardsystemer. Et OT-system er som oftest designet for å driftes frittstående, men blir nå mer og mer integrert og tilkoblet både internt på skipet og ekstern mot landbaserte installasjoner. Selv om sannsynligheten for å bli utsatt for angrep er ansett som lav, er det forbundet en risiko med at systemene er kritisk for skipsdriften. DNV vurderer det derfor at

det er «behov for industrispesifikke retningslinjer for IKT-sikkerhet for OT-systemene om bord.»

I Meld St 10 «risiko i et trygt samfunn» (Regjeringen, 2016) beskriver regjeringen en ønsket organisering av cybersikkerhet i Norge. Det anbefales en overordnet Computer Emergency Response Team (CERT) (NSM, 2018b) som skal ha et koordinerende ansvar opp mot mindre cyber sektorielle respons miljøer (SRM) (NSM, 2018b). De sektorielle respons senterne vil i noen tilfeller være knytte sammen flere næringer med felles interesser for å ivareta deres digitale sikkerhet. Denne organiseringen er tenkt å ivareta primært norske virksomheters behov for støtte i forbindelse med digitale angrep. Dette må da sees i den konteksten at digitalsikkerhet er en virksomhets eget ansvar, men at myndighetene kan til en viss grad assistere virksomheter som blir angrepet. Det gjelder da primært virksomheter som har tjenester eller funksjoner som faller inn under sikkerhetslovens mandat (Sikkerhetsloven, 2019).

I Sjøfartsdirektoratets strategi for maritim cybersikkerhet defineres «Maritim digital sikkerhet omfatter håndtering av risiko, sikkerhetsmessige utfordringer og vurdering av konfidensialitet, integritet, tilgjengelighet knyttet til de digitale systemer som er nødvendig for sikker seilas, drift, operasjon, og systemer for håndtering av informasjon om fartøy, last og personer om bord.»(SDIR, 2020).

Denne definisjonen omfatter med andre ord all informasjon, alle systemer ombord og all kommunikasjon til og fra skipet. Definisjonen favner også om systemer som kan direkte eller indirekte påvirke seilas, drift og operasjon av skip, havner og farled i negativ grad. Domenet er ganske omfattende, og systemer og prosesser er mange. I denne konteksten omfatter dermed maritim næring så mye mer, enn hva vi ser på i konteksten av innføringen av IMOs cybersikkerhetskrav.

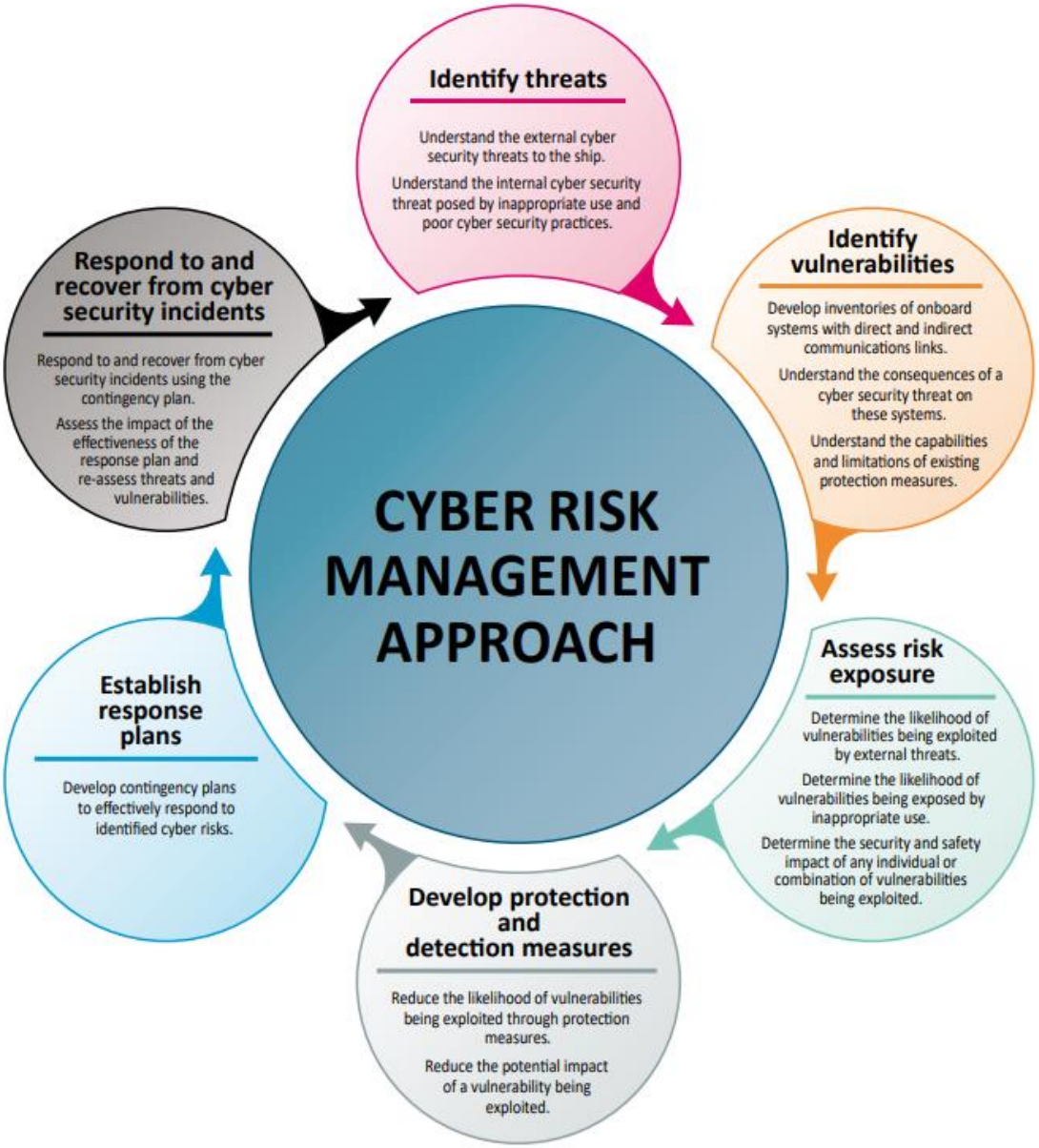


Figur 2

I figur 2 har jeg laget en figur som skal visualiseres Sjøfartsdirektoratets definisjon av maritim cybersikkerhet, og hvor omfattende den er i forhold til IMOs cybersikkerhetskrav til maritim næring, samtidig som de knyttes tett sammen av infrastruktur og kommunikasjonssystemer. Blå sirkel viser fartøy og rederi som er omfattet av IMOs cybersikkerhetsresolusjon. Brun sirkel viser kritisk infrastruktur som samhandler med fartøy og rederier. Til slutt så viser den tynne mørkeblå sirkelen i randsonen mellom blå og brun sirkel de ulik systemene som fasiliteterer for samhandling mellom de ulike partene.

2.2 IMOs cybersikkerhetsresolusjon for maritim næring

NTNU professor Georgios Kavallieratos(Kavallieratos, 2022) ved NTNU sa at «*Jo mer sammenknyttet infrastrukturen er, jo mer sårbar er den for digitale angrep*». IMO resolusjonen for cybersikkerhet har sammenstilt et sett med regler som fartøy og rederi skal etterleve for å øke den digitale motstandskraften. Resolusjonen beskriver hvilke prosesser som skal ivaretas innen digital sikkerhet. Men definerer ikke en proprietær standard eller metode slik som NIST (NIST, 2023b) eller ISO 27000 (ISO, 2023) som skal benyttes for å møte kravene.



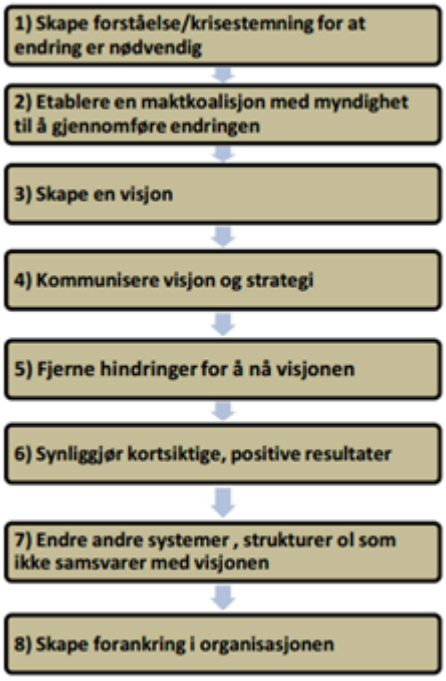
Figur 3. BIMCO, The Guidelines on cyber security onboard ships(BIMCO, 2020)

Figur 3 viser de ulike stegene som må adresseres av rederi eller fartøy for å ha en helhetlig tilnærming til maritim cybersikkerhet. Bimco modell(BIMCO, 2020) beskriver de ulike trinnene med tilhørende mål for delprosessene. Modellen presenterer en metodisk tilnærming til trusselvurdering, egen sårbarhetsanalyse og utvikling av handlingsplaner for å møte et eventuelt angrep. Et viktig overordnet moment som Bimco belyser er at det er viktig å ha

balanse mellom beskyttelses tiltakene og handlingsplanene for å skape et resilient sikkerhetssystem. Et annet moment er at Bimco's «Cyber risk management approach» ikke er en engangsprosess, men en kontinuerlig revideringsprosess for å ha oppdaterte og adekvate beskyttelsestiltak og handlingsplaner.

2.3 Kotter

Professor Kotter (Kotter, 1995) har utviklet teoriene knyttet til det vi på norsk kaller endringsledelse. Han har utviklet en modell på åtte trinn for hvordan en virksomhet bør gjennomføre en omstilling for å oppnå en vellykket transformasjon.



Kotter, John (Kotter, 1995)

Det første trinnet i endringen er å skape og kommunisere et budskap preget av viktighet og prioritet. Skal man lykkes med å skape endring, må man sette i gang framfor å sitte for lenge på stubben og analysere.

I trinn to fokuserer man på å etablere et styrende team for transformasjonen. I en organisasjon kan dette være formelle og uformelle ledere, mens i ei næring vil man gå på tvers av sektoren og inkludere både ansvarlige etater, bransjeorganisasjoner, rederi og virksomheter som har en indirektes rolle i omstillingen.

Deretter må man i trinn tre formulere en visjon som gir de som skal omstilles et bilde av hva endringen skal oppnå. Man skal kunne skimte en visjon, men den skal ikke ha full oppløsning med mange detaljer.

I trinn fire skal man kommunisere visjonen og strategien for omstillingen. Hvordan formidle dette til interessentene er et meget aktuelt spørsmål å stille seg. Har man tilstrekkelig med insentiv til å kunne få framdrift i endringen, eller må man finne fram den klassiske pisk eller gulrot dreieboka.

I trinn fem fjernes hindringer for å nå visjonen. Ofte eksemplifiseres dette med typiske personligheter som kan oppfattes som motstand eller pådrivere for endringene og må enten omplasseres eller fjernes. I konteksten av en endringsreise kan det også være systemer i organisasjonen som må skiftes ut for å få realisert gevinsten av endringen.

Når omstillingen kommer til trinn seks er det viktig å skape kortsiktige positive resultater. Dette veikartet med mellomliggende mål er med på å skape både målbare faser, men også beskrive etapper som gir deltakerne i omstillingen en tilbakemelding på resultat. I en omstilling av en markedsstyrt næring vil synliggjøring av verdiskapning i form av nøkkeltall i kvartalsvis rapportering og publisering av årsrapporter være hensiktsmessig.

I trinn sju skal man endre systemer som påvirker omstillingen på en negativ måte, slik at det å nå visjonen skal bli en varig tilstand. Selv om et cyberrelatert prosjekt ofte knyttes til maskiner og servere, så er det ikke ekskluderende for organisasjonsendringer eller prosedyreendringer.

Til slutt spikres omstillingen slik at den oppnår varighet. Permanente strukturer forankres, samarbeidsavtaler på tvers av næringen signeres og verdiskapningen fortsetter.

De åtte stegene for en vellykket omstilling av en organisasjon, er en prosess med å endre menneskets adferd. Endring av atferden er det overordna fokuset, men er også finne igjen i alle trinnene. Kotter (Kotter, 1995) beskriver det som den mest krevende delen av en omstilling. Mennesket kan være motvillig til forandring, så av den grunn er det viktig å få på plass en solid forankring samtidig som at man klarer å holde fokus på både målet og tempoet i endringen.

En utfordring med Kotters teori er at den framstå som ei smørbrødliste over hva som skal gjøres, men har lite oppløselighet på innholdet i trinnene. En slik framstilling av endringen kan fort fremstå som en oppskrift som ledere bare skal trekke gjennom, og sier lite om hva som skal gjøres på de forskjellige trinnene.

Kotters teori kan sies å være framstilt som en åtte trinns prosess, med et noe forenkla innhold i hvert av de åtte trinnene. Selve omstillingen er avhengig av å endre menneskenes atferd, men modellen sier lite om de psykologiske mekanismene som må på plass for å holde mennesket motivert og omstillingsvillig gjennom hele omstillingsprosessen.

Modellen har positive sider ved at den skaper engasjement blant virksomhetens tilsatte. Den har tydelige trinn som gjør navigasjon lettere og modellen er tilpasset en tradisjonell hierarkisk organisasjon. De vanligste utfordringene med denne modellen er at den er drevet i en top-down prosess, med lite påvirkning fra organisasjonen som helhet. Og at den i liten grad gir rom for den enkelte tilsattes emosjonelle behov når de blir utsatt for en slik transformasjon. En omstilling av en hel næring vil derfor bli utfordrende, da det i hver underordet organisasjon må påberegnes en eller annen form for endringsreise for å implementere løsningen lokalt.

Til slutt er det viktig å huske på det kjente sitatet fra John Kotter “Transformation is a process, not an event.” Denne refleksjonen er med på å belyse at transformasjonen er en vedvarende aktivitet, og ikke bare en ting man gjør i et begrenset tidsrom med definert tid og rom. Næringen vil i fremtiden bli tvunget til å drive sin tradisjonelle verdiskapning, parallelt med at de endrer seg for å kunne være relevant. Et slikt to-spann vil kreve mye av de tilsatte og organisasjon som helhet, både om man er direkte eller indirekte berørt av transformasjonen.

3 Metode

I dette kapittelet beskrives en detaljert plan for hvordan studien min er designet for å besvare min problemstilling og mine forskningsspørsmål. Metode kommer av det greske «methodos», som betyr å følge en bestemt vei til målet (Johannesen, 2021). I de påfølgende kapitlene er avsnittene er valgt metode brutt opp i forskningsdesign, kvalitativ metode, utvalg av informanter, datainnsamling, databehandling og analyse, dataanalyse, validitet, reabilitet og etiske problemstillinger. Metodekapittelet beskriver hvordan mitt veikart gjennom forskningsprosessen skal hjelpe meg med å navigere stødig til målet og bevare integriteten i studien min.

3.1 Forskningsdesign

Mitt valg av forskningsdesign har som utgangspunkt å få undersøkt problemstillinga best mulig. Jeg har studert implementeringsarbeidet i forbindelse med innføringen av IMO resolusjonen for cybersikkerhet på de ulike nivåene i næringen, og har derfor valgt et forskningsdesign som gir meg en eksplorerende innfallsvinkel til tema. Jeg har henta inn mye informasjon fra et lite antall informanter på alle nivåer i næringen, og har en problemstilling som er formulert slik at den søker en deskriptiv analyse. Problemstillingen min har jeg konstruert for å kunne gjøre funn som kan gi en overføringsverdi til videre implementeringsarbeid av cybersikkerhet i maritim næring, og ikke frambringe statistikker som kan gi mer generelle betraktinger i forhold til implementeringsarbeid og endringsledelse.

Forskningsdesignet beskrives som «kartet som viser veien til målet». Jeg har delt forskningsprosessen inn i ulike, og klart definerte faser. Jeg har prøvd å oppnå en effektiviseringsgevinst ved hjelp av å bruke en parallell og integrert faseplan, men i og med at flere av fasene knyttet til intervju og analyse av data er sekvensielle så valgte jeg å gjennomføre de suksessivt. De ulike fasene er; studie av sekundærdata, utvikle intervjuguide, gjennomføre intervjuer, strukturere innsamlede data, analyse og konklusjon.

Jeg valgte et eksplorativt forskningsdesign der jeg først samla inn sekundærdata for å få en teoretisk forståelse for fagområde og teori. Deretter intervjuet jeg mine informanter for å verifisere min problemstilling, og forhold vedrørende forskningsspørsmålene. Innsamling av

sekundærdata er den fasen av forskningen omfattet både kunnskapsinnhenting om tema IMO MSC.428(98), samt innsamling om forskning og teorier som er relevant for tema.

3.2 Kvalitativ metode

Forskningen har benyttet en kvalitativ metode, der jeg intervjuet informanter fra forskjellige nivåer innen norsk maritim næring. Det vil si politisk, strategisk, operasjonelt og taktisk nivå. For å lykkes med dette intervjuet jeg følgende; en politiker på Stortinget, en informant fra Sjøfartsdirektoratet som utøvende etat på strategisk nivå, en informant fra Nasjonal Sikkerhetsmyndighet som er en utøvende etat knyttet til cybersikkerhet, en representant fra Rederiforbundet på operasjonelt nivå. Jeg ønsket å intervjue flere informanter på taktisk nivå, men de lot seg ikke rekruttere.

Et mål i forskningen min var å avklare mål og forventninger fra både forvaltende og utøvende nivå. Ved hjelp av en god litteraturstudie i forkant av intervjuene, har jeg funnet informanter som er representativ for de ulike nivåene. Et implisitt krav til informantene har vært at de er kjent med eller jobber direkte med maritim cybersikkerhet, og IMO MSC.428(98)(IMO, 2017).

En begrensning ved dette tema er at flere av de aktuelle informantene var enten i ferd med å operasjonalisere IMO MSC.428(98)(IMO, 2017) for sin virksomhet eller nivå, eller så var kjennskapen deres primært knyttet til et overordnet nivå av cybersikkerhet.

Forskningsdesignet har vært eksplorativt da problemstillingen er fremstår som noe som ikke enkelt kan kvantifiseres eller sammenliknes. Informantene som jeg rekrutterte befant seg i både næringsliv og forvaltning, noe som gav ulike perspektiver fra ulike nivåer.

Mitt valg av å bruke kvalitativ metode, samsvarte godt med mitt eksplorative design. Både gjennom den innledende litteraturstudie og intervju med informantene opplevde jeg å få en dypere, men ikke kvantifiserbar forståelse for hvordan forskningstema påvirker alle deler av næringen. Bruk av intervju gav meg også tilstrekkelig frihet til å følge opp mottatt informasjonen med oppklarende spørsmål til informantene.

3.3 Utvalg av informanter

Med utgangspunkt i det valgte forskningsdesignet prøvde jeg å rekruttere en mest mulig diversifisert gruppe med informanter. Intervjuobjektene er valgt ut i fra knytning til næringen, samt inngripen i digital sikring knytte til maritime problemstillinger. På politisk og strategisk nivå benyttet jeg kriteriebasert rekruttering av informanter. Utvalgsmetoden jeg benyttet hadde til intensjon å rekruttere informanter som oppfyller bestemte forhåndsdefinerte kriterier (Johannesen, 2021). I dette tilfellet var kriteriene at informanten skulle gi innblikk i politiske og/eller etatsprioriteringer knyttet til innføringen av IMO konvensjonen. Informantene tilførte forskningsprosessen en unik bredde og helhetsforståelse for nasjonale politiske og faglige prioriteringer knyttet til forskningstema, og etter min oppfatning tilførte informantene min forskning god innsikt i myndighetenes planer og prioriteringer.

Ved valg av informanter på operasjonelt og taktisk nivå prøvde jeg å benytte en utvalgsstrategi som skulle gi maksimal variasjon. Utvalgsstrategien beskrives som «når forsker har etablert det typiske eksempel, så leter han etter det som speiler det ekstreme (Johannesen, 2021). Ved å benytte denne strategien ønsket jeg å få innsikt i bredden av løsninger som er implementert på operasjonelt og taktisk nivå.

Planen min med tanke på rekruttering av informanter på taktisk nivå gikk ikke i orden. Etter et om lag et halvt år med forsøk på å rekruttere informanter besluttet jeg at å gå videre med min forskning uten å intervjue informanter på taktisk nivå. Jeg oppnådde derfor ikke det ønskede kildegrunnlaget for min forskning. Men takket være at min informant på operasjonelt nivå hadde god innsikt i hva som skjer både ombord på fartøy og i rederiene, fikk jeg fanget opp en del av nyansene fra de i næringen som har skoen på.

Tabell 1 viser en oversikt over mine informanter og på hvilket nivå i norsk maritim næring de tilhører.

Nivå	Etat/organisasjon	Antall
Politisk	Stortingspolitiker	1
Strategisk	Sjøfartsdirektoratet/NSM	2
Operasjonelt	Norma Cyber	1

Informanten på politisk nivå er en Stortingspolitikker som sitter i Finanskomiteen, samt partiets beredskapsutvalg. Personen har jobbet innen sikkerhetsbransjen i om lag tjue år, og med cybersikkerhet i privat sektor i ti år.

Kilden fra Sjøfartsdirektoratet er en erfaren seksjonsleder, med tung teknisk utdannelse. Har vært sentral i utviklingen av Sjøfartsdirektoratets strategi for maritim cybersikkerhet.

Informanten i NSM er en seksjonssjef som har erfaring fra både privat og offentlig cybersikkerhet. Personen er ikke ekspert på maritim cybersikkerhet, men har god kjennskap til NSM og deres prioriteringer og hjemmelsgrunnlag.

Kilden fra Norma Cyber er teknisk utdannet, og meget erfaren inne maritim cybersikkerhet.

3.4 Datainnsamling

Datainnsamlingen i min forskning var kvalitative intervju. Jeg valgte denne formen for datainnsamling for å få informanten til å føle seg fri til å svare det han/hun opplever som viktig og riktig svar på spørsmålene (Johannesen 2021).

Jeg produserte en intervjuguide for å beskrive mål og hensikt med undersøkelsen. Spørsmålene tilstrebes å være åpne, og oppmuntre til dialog mellom forsker og informant (Johannesen 2021).

Selve intervjuguiden og spørsmålsskjema var likt for alle informantene. Jeg stilte informanten spørsmål og hadde samtidig muligheten til å stille oppklarende spørsmål knytta til svarene fra informanten. Denne formen for datainnsamling var godt egnet siden jeg ønsket å oppnå en fyldig og detaljert beskrivelse av informantens forståelse, følelser, erfaringer, oppfatninger, meninger, holdninger og refleksjoner knyttet til et fenomen(Johannesen, 2021).».

3.5 Databehandling og analyse

Det er viktig at forskeren som samler inn dataene, også er den som analyserer og tolker dem, fordi teorier, hypoteser og forskerens forståelser er viktige utgangspunkt for å forstå dataanalysen (Silverman, 2006).

Jeg er alene om å skrive min masteroppgave. Av den grunn er det jeg som har alle rollene innen databehandling og analyse.

Innledningsvis gjennomførte jeg en studie av sekundærdata for å få et bedre bilde av fagområde, og for å kunne utvikle et intervju med gode spørsmål og en egnet intervjuguide.

Etter at intervju var fullført, sammenfattet jeg intervjuene i sammendrag. Analysen av data består av to faser. Den ene er å organisere data, og den andre er datareduksjon, analyse og tolke de innsamlede data (Johannesen, 2021).

Som en del av min litteraturstudie utviklet jeg intervju og intervjuguide, der jeg trakk ut nøkkelord som kunne være med på å indeksere datamengden som en del av en tverrsnittbasert inndeling. Nøkkelordene var også nyttige til å tematisere intervjuene for å skape relevante spørsmål.

3.6 Dataanalysen

Hensikten med min dataanalyse var å analysere og sammenligne data for å forstå informantens mening vedrørende mitt forskningstema. I og med at jeg intervjuet informanter basert på maksimal variasjon med påfølgende analyse, så forventet jeg en viss spredning i rådatafangsten.

Dataanalysen hadde som fokus å redusere tekstmengden til analyserbar data. Dette gjorde jeg gjennom å kategorisere data med utgangspunkt i de kategoriene som jeg har tatt med meg fra gjennomgang av sekundærdata.

Kategoriseringen ble gjennomført sekvensielt etter hvert intervju, derfor tok jeg høyde for ekstra analysearbeid med alle intervju etter hvert som nye kategorier oppstår. Denne metoden kan fremstå som tungvint, men var meget nyttig når intervjuene presenterte tematikk som jeg ikke hadde tatt høyde for når jeg startet mine intervjuer.

Etter at jeg var ferdig med å kategorisere intervjuene knyttet jeg kategoriene opp mot Kotters teori for endringsledelse, med fokus på trinn fem til og med åtte.

3.7 Validitet

Validitet beskrives av hvor gyldige dataene er (Johannesen, 2021). Validitet deles inn i troverdighet og overførbarhet.

Troverdighet, også kalt intern validitet, omtales som «måler vi det vi tror vi måler?»(Johannesen, 2021). I kvalitative undersøkelser måler man i hvilken grad forskerens fremgangsmåte og funn på en riktig måte reflekterer formålet med studien og representerer virkeligheten (Johannesen, 2021).

Et annet aspekt av validitet er det som kalles overførbarhet eller ekstern validitet. Kan forskningen min innen maritim cybersikkerhet overføres til andre bransjer? Jeg har underveis prøvd å generalisere funnene mine på en måte som gjør at funnene kan for eksempel anvendes innen forskning på sektorprinsippet.

Dette forskningsarbeidet har få, men sentrale informanter innen cybersikkerhet. Intervjuene fanger opp mye informasjon om samme tema, men med ulikt fokus på grunn av kildenes plassering i hierarkiet og nivåer. Dermed blir det samlet inn mye data fra ulike nivåer, som gir et nyansert bilde av tema.

3.8 Relabilitet

Relabilitet – knyttes til hvilke data som er blitt samlet inn, brukt og bearbeidet. Relabilitet knyttes primært til kvantitativ metode, der det er utviklet spesielle tester for å måle relabilitet (Johannesen, 2021).

Jeg har satt søkelys på informantens subjektive framstilling av sine erfaringer knyttet til mitt forskningstema. I designet mitt har det vært viktig at spørsmålene som har vært stilt til informanten gitt rom for både å samle inn positive og negative erfaringer knyttet til tema, slik at jeg har fått et representativt bilde av informasjonen. Det var særlig viktig for informanter på strategisk og operasjonelt nivå, da det var de som i størst grad kunne informere om praktiske erfaringer knyttet til innføringen av IMO konvensjonen.

I og med at jeg i forskningen min prøver å gi svar på hvordan implementeringen av konvensjonen vil utvikle seg, er erfaringene til de som har «skoen på» viktige data å samle inn. Gjennom å bruke utvalgsstrategien maksimal variasjon så har jeg i min forskning prøvd å

gi et mer holistisk bilde av erfaringene, noe jeg har til dels lykkes med i forhold til strategisk og operasjonelt nivå.

En utfordring knyttet til min forskning og reabilitet er at jeg ikke fikk rekruttert informanter på taktisk nivå. Dette nivået er i stor grad de som er det utførende leddet i implementeringen av IMOs cyberresolusjon. I etterkant av min datainnsamling så sitter jeg igjen med at min informant på operasjonelt nivå i stor grad gitt meg innblikk i hvordan erfaringene på taktisk nivå er. Dette fordi informanten sitter i en teknisk stilling som representerer en stor del av de norske rederiene og frakte flåten.

3.9 Etiske problemstillinger

Masteroppgaven har primært bestått av kvalitative intervjuer, og det er jeg som forsker som har det etiske ansvaret opp mot de involverte informantene. For å få forståelse for fagområdets kompleksitet så har jeg lest i ressursbiblioteket til De nasjonale forskningsetiske komiteene(Fangen, 2015) for å få belyst etiske problemstillinger som kan bli aktuelle for min forskning. De trekker fram følgende tre kategorier som må vies oppmerksomhet.

Informert samtykke: Det betyr at de som skal delta, skal ha nødvendig informasjon om undersøkelsen. Informanten mine har samtykka skriftlig i forkant.

Konfidensialitet beskrives av De nasjonale forskningsetiske komiteene som «Forskere skal behandle innsamlet informasjon konfidensielt hvis det er avtalt. Hvis forskere skal bruke informasjon som er samlet inn av andre under taushetsplikt, må de sikre at det foreligger fritak fra denne taushetsplikten» (Fangen, 2015). Konfidensialiteten har vært en viktig del av tilliten mellom informanter og forskningen min, og det har vært viktig at løfter om fortrolighet og videreformidling overholdes.

Datainnhenting basert på bruk av kvalitative intervju har medført behandling av personopplysninger, noe som betyr at jeg har meldt forskningsprosjektet mitt til Norsk senter for forskningsdata (NSD). Prosjektet ble meldt inn i som en del av utviklingen av intervju og intervjuguide.

Forskningen har brukt elektronisk lydopptaker i samsvar med Nord Universitets retningslinjer og retningslinjer for personvern. Før intervju har jeg informert informanten om

intervjuet og vedkommende har signerer samtykkeskjema. Etter data er sammenfattet, slettes opptak. I invitasjonen til informantene har jeg gitt informantene informasjon om personvern og databehandling, slik at informantene har kontroll på sin anonymitet.

4 Empiriske funn

Funnene som presenteres under er hentet fra intervjuene som er gjennomført med mine informanter på politisk, strategisk og operasjonelt nivå. Strukturen på presentasjonen vil knyttes til de fire mest framtredende temaene; kompetanse, næringens forståelse for oppdaget, sektorielt ansvar og veien videre.

4.1 Kompetanse

Informantens svar på mine intervjuer viser at det er en generell mangel på utdannet personell innen cybersikkerhet. Samtlige kilder trekker frem at det ikke utdannes nok personell med kompetanse innen cybersikkerhet i Norge, til å dekke behovet som etterspørres. Og ser man deretter på spesialisering innen maritim cybersikkerhet, er gapet mellom behov og produksjon enda større.

Kompetanseproblematikken adresseres fra mine informanter som et to-delt problem. På den ene siden er det liten tilgang på teknisk personell som er utdannet innen cybersikkerhet som spesialfelt. Mens på den andre siden er operativt og teknisk personell ombord på fartøy i liten grad utdannet innen cybersikkerhet gjennom sin maritime utdanning, enten det er på maritim fagskole eller høyskole. Stortingsrepresentanten poengterer denne problemstillingen, og predikerer at den kommer til å vedvare frem til kunstig intelligens (KI) i større grad kan fylle kompetansehullet for teknisk personell i kontrollsentre. Informanten i Sjøfartsdirektoratet belyser på den andre siden at etaten har siden innføringen av IMO resolusjonen gjennomført en informasjonskampanje for å heve bevisstheten vedrørende maritim cybersikkerhet og kravene som innføres i forbindelse med IMO-resolusjonen.

Informanten fra Sjøfartsdirektoratet forteller at de siden implementeringen av IMO resolusjonen startet har drive et stort opplysningsarbeid, både mot besetninger og rederier i den hensikt å heve forståelsen for både trusselen og tiltakene som reduserer den. Dette arbeidet har hatt som mål å få maritim cybersikkerhet på agendaen i styrerommet, samt gjøre fartøysbesetningene kjent med utfordringer og løsninger knyttet til hendelser generert av et cyberangrep.

Informantene i både Sjøfartsdirektoratet og Norma Cyber beskriver at personellet ombord på fartøyet som skal ha rollen som fartøyets cybersikkerhetsansvarlige vil i de fleste tilfeller ha

det som en oppgave, og ikke som stilling ombord. Informanten fra Norma Cyber beskriver at oppgaven stort sett faller inn under skipselektrikers oppgaver der fartøyet ha egen elektriker. På mindre fartøyer tilfaller oppgavene knyttet til cybersikkerhet i skipssjef, mens fartøy med større bemanning kan i noen tilfelle ha egen Chief Information Security Officer(NIST, 2023a) ombord.

Informanten på operasjonelt nivå erkjenner utfordringen knyttet til kompetent bemanning innen cybersikkerhet i næringen, men beskriver samtidig en bransje som ikke lar seg definere av nasjonale utdanningsprioriteringer de siste årene. Det beskrives en hverdag der outsourcing av backoffice tjenester er å regne som normalen, der cybersikkerhet løses fra bedrifter i andre verdensdeler. En løsning som gjør rederi og fartøy mindre sårbare i forhold til flaggstatens prioriteringer i forhold til utdanning. Informantene på både politisk og operasjonelt nivå beskriver en bransje som er meget merkantil og selvdrevet når det kommer til å levere tjenester som imøtekommer kravene som stilles fra myndighetene. Det poengteres også at bransjen i liten grad er avhengig av incentiver og myndighetskrav for å implementere nye krav til næringen, noe som etableringen av Norma Cyber er godt eksempel på.

Informanten fra Nasjonal Sikkerhetsmyndighet(NSM) adresserer at maritime virksomheter som har leveranser som reguleres av Sikkerhetsloven vil ha begrensninger knyttet til outsourcing av sin virksomhet, enten det knyttes til geografisk lokalisering av underleverandør eller krav til nasjonalitet på personellet som betjener systemene, og nevner at NSM har etablert et system av godkjente nasjonale cybersikkerhetsvirksomheter som kan hjelpe berørte virksomheter i å etablere gode cybersikkerhetsrutiner og hendelseshåndtering ved angrep.

Informanten fra NSM poengterer også at å skaffe kompetent personell til å bemanne sektorielle responssenter (NSM, 2018a) eller CERT'er(NIST, 2023b) er utfordrende, særlig fra et statlig ståsted der det private næringslivet i stor grad kan tilby kompetent personell bedre vilkår. Noe som gir lav ståtid blant kompetent personell, som deretter påvirker etableringstiden av operasjonssenter og fagmiljøer.

Ingen av informantene kjente til målrettet eller spesialisert utdanning, og mente at spisset kompetanse må etableres både som en del av den maritime fagutdanningen, og som en del av de tekniske utdanningene.

4.2 Næringens forståelse for oppdaget

Samtlige informanter opplever at de berørte aktørene i den maritime næringen har en god forståelse for viktigheten av IMO resolusjonen, samt hva den krever av deres organisasjon. Med ulik ordlyd forteller informantene at implementeringshastigheten i større grad preges av rederiets egne prioriteringer i forhold til hvor fartøyene seiler, og når kontroller er tidfestet.

Informanten fra NORMA Cyber forteller om en maritim næring som tar cybersikkerhet på alvor, særlig etter flere angrep på norske aktører de siste årene, som har hatt stor konsekvens for de berørte partene. Han forteller at selv om mindre og spesialiserte fartøyer faller utenom mandatet fra IMO resolusjonen, så har han et inntrykk av at også de fartøyene prøver å implementere resolusjonens innhold for å øke fartøyets og rederiets resiliens mot cyberangrep.

Samtlige informanter er positiv til innføringen av IMOs cybersikkerhetsresolusjon. Den er med på å sette maritim cybersikkerhet på agendaen både for Norge som nasjon, og den maritime næringen som en berørt part.

Mine politiske og strategiske informanter beskriver innføringen av kravene som et godt utgangspunkt for å gjøre den norske flåte robust i forhold til digitale angrep. Der bevisstgjøringen om trusselen, etablering av digitale sikkerhetsrutiner om bord og beredskapsplaner vil i stor grad utgjøre en forskjell om fartøy eller rederi skulle bli utsatt for et digitalt angrep.

Informanten på operasjonelt nivå forteller at selv om resolusjonen er signert av nasjonene som utgjør IMO, så tolkes innholdet i resolusjonen ulikt fra land til land. Dermed blir etterlevelse av kravene i stor grad påvirket av flaggstatens prioriteringer.

Sjøfartsdirektorat informanten forteller også at IMO standarden ved første gjennomgang kan virke som en enkel og grei ramme for cybersikkerhet, men når man setter seg inn i dens innhold så stiller den tydelige krav til både digital infrastruktur om bord, kompetanse blant

skipets besetning og konkrete handlingsplaner for håndtering av angrep både om bord på fartøy og hos rederiet.

Informanten fra NORMA Cyber forteller at større rederier outsourcer oppgaver knyttet til IT-drift til andre nasjoner på grunn av lite tilgang på IT-utdannet personell i Norge. Og at det over tid har vært løst ved at «backoffice» tjenester for rederier befinner seg for eksempel i Singapore, der rederiets cybersikkerhetsoppgaver er kontraktsfestet. På den måten blir IMO resolusjonen noe som en tredjepart forholder seg til.

Sjøfartsdirektoratet forteller at cybersikkerhet blir forvaltet som en del av ISM-koden (International Management Code for the Safe Operation of Ships and for Pollution Prevention)(SDIR, 2014). Det vil si at fartøyer inspiseres regelmessig for å kontrollere at de følger gjeldende forskrifter. Sjøfartsdirektoratet forteller at første året som IMO-resolusjonen ble implementert, ble kravene knyttet til cybersikkerhet først og fremst brukt som et veilednings grunnlag, men fra og med 2023 så sanksjoneres avvik med pålegg om utbedring av avvik til rederiet.

Informantene fra Sjøfartsdirektoratet og Norma Cyber trekker frem at det primært er rederiets ledelse som driver frem implementeringen av IMO resolusjonen, men at ansvar og oppgaver i stor grad tilfaller nøkkelpersonell om bord på fartøy. Ombord på mindre fartøy så vil oppgaven tilfalle teknisk eller sikkerhetspersonell, mens på større fartøy så kan man sågar ha et eget besetningsmedlem med hovedoppgave å ivareta fartøyets cybersikkerhet.

4.3 Sektorielt ansvar

Forskningen har samlet mine informanters svar vedrørende det sektorielle ansvar. Med det mener jeg svar som reflekterer på hvordan området er organisert både med tanke på krav og kontroll, men også samvirke med andre bransjer i næringen og tanker vedrørende etablering av et sektorielt responssenter.

Mine informanter belyser en bransje i utvikling når det gjelder maritim cybersikkerhet. Samtlige informanter erkjenner at det har vært en sårbar næring som har opplevd cyberangrep de siste årene. Der samtlige informanter har enten vært direkte eller indirekte vært involvert i krisehåndteringen og driftskontinuiteten ved blant annet Vard skipsverft (Executive, 2020).

Informanten i Sjøfartsdirektoratet forteller at det i starten av 2023 ble besluttet å etablere et sektorielt responssenter for maritim næring som skal utvikles og driftes av Kystverket. Responssenteret ledes av Kystverket, uten bidrag fra andre deler av den maritime næringen. Et sektorielt ansvar som omfavner både Sjøfartsdirektoratets innenriks og utenriksfartøy, samt bemannede og ubemannede installasjoner langs kysten. Informanten ytrer misnøye med at det sektorielle responssenteret ikke blir et felles operasjonssenter bemannet av representanter fra alle bransjer i næringen.

På operasjonelt nivå forteller informanten at selv om det etableres et sektorielt responssenter for næringen hos Kystverket, så vil deres mandat være å støtte fartøy som primært seiler i norsk farvann. Det poengteres at responssenteret ikke har et mandat til å støtte fartøy som løser oppdrag i internasjonale farvann. Da dette er en stor del av den norske fartøysflåten, vil ikke etableringen av et responssenter kunne erstatte Norma Cyber oppdrag.

Informanten fra NSM utleder at etaten har noe kapasitet til å støtte den maritime næringen, men at NSMs fokus primært er rettet mot forebygging og håndtering av cyberhendelser som oppstår hos norske virksomheter som er underlagt sikkerhetsloven. De kan til en viss grad hjelpe andre aktører, men at de som oftest sendes videre til NSM partner(NSM, 2020) virksomheter for cybersikkerhet.

På operasjonelt nivå ytrer informanten lite meningen om organiseringen av det sektorielle responssenteret, da de som paraplyorganisasjon for en stor del av aktørene i bransjen ikke er i et kommandoforhold til responssenteret. De presiseres at de leverer tjenester til en selvgående bransje, som fram til nå har løst oppdraget på vegne av sine kunder uten et kommandomessig forhold til resten av statsapparatet i Norge.

Informantene på både politisk og operasjonelt nivå beskriver en maritim næring som er meget handlekraftig og ressurssterk. Den politiske kilden adresserer også at næringen er kjent for å være kostnadsfokusert, noe som materialiserer seg i at det spares på det som oppleves som å falle på utsiden av kjernevirksomheten. På den andre siden belyser informanten ved Norma Cyber at det innen bransjen finnes alle nyanser av prioriteringer av cybersikkerhet. Og at fokuset oftest kan relateres til hvor eksponert og konfliktnært rederiets fartøyets operasjoner befinner seg.

Informanten på politisk nivå beskriver de sektorielle cybermiljøene som uegnet for å løse oppdaget knyttet til digital sikkerhet i Norge. Han tar til orde for at staten i større grad samler den digitale sikkerheten i en etat, som har til oppdrag å håndtere cyberhendelser som berører Norge. Denne organiseringen vil i større grad kunne frigjøre ressurser og etablere et robust fagmiljø, istedenfor mange små. Informanten fra NSM understøtter dette til dels når han beskriver dagen samhandling mellom etatene som vellykket på et teknisk nivå, men fortsatt ikke effektivt når det kommer til operativ samhandling.

4.5 Videre implementering

Informantene enes om at det er viktig at myndighetene følger opp sine oppgaver knyttet til å informere om standarden og kontrollere at den implementeres gjennom inspeksjoner. Informantene på politisk og operasjonelt nivå poengterer viktigheten av at det standarden tar hensyn til fartøyet og eventuelt rederiets størrelse slik at implementeringen ikke blir så kostnadsdrivende at mindre rederier må melde oppbud.

Informanten ved Norma Cyber tok opp at nyere fartøy har større angrepsflater, enn eldre. Noe han eksemplifiserte med økningen i antall nettverksporter på et fartøy fra 2010 i forhold til et fartøy som tas i bruk i dag. Det er da snakk om en tredobling av antall nettverksporter. I den sammenheng tok informanten til orde for at eldre fartøy ikke skulle ha samme krav til cybersikkerhet, da det ville medføre større kostnader i forhold til å radikalt utvide og endre nettverksarkitekturen og kapasiteten om bord. Og at myndighetene heller så på hvordan etterleve IMO kravene i mer moderne og autonome fartøyer.

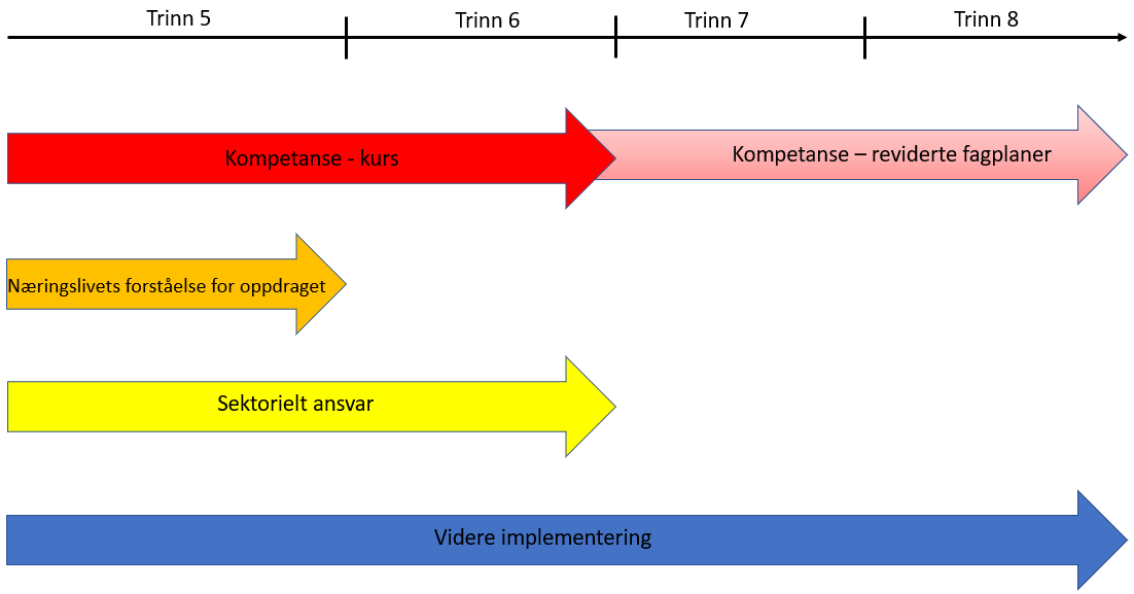
NSMs informant tok opp at staten som aktør i større grad burde stille krav til cybersikkerhet i forbindelse med utlysning av kontrakter. I og med at det er mange og store kontrakter som privat næringsliv leverer til staten, så kommer krav til leverandørens cybersikkerhet til å være en viktig del av leveransen gjennom statens standardavtaler. Informanten synes dette i prinsippet er positivt, men er uroa for at det kan i større grad kan bli «compliance» til kravene. Uroen er at det blir et fokus på å tilfredsstille de formelle kravene, og ikke gjøre det til en operativ prosess. Dermed blir ikke sikkerheten nødvendigvis bedre, men det ser pent ut på papiret.

5 Analyse av funnene i en Kottersk kontekst

Jeg har analysert mine funn opp mot min valgte teori, der jeg har tolket for å belyse, og besvare oppgavens problemstilling. Analysen min er av den grunn orientert opp mot Kottes åtte trinnsmodell for endringsledelse. Forskningens fokus har vært knyttet til trinn fem til og med åtte. Kotters trinn er trinn 5: fjerner hindringer, trinn 6: skape og planlegge hurtige og synlige resultater, trinn 7: konsolidere endringene for å skape momentum og trinn 8: forankrer endringene i bedriftskulturen og institusjonaliserte de nye holdningene i virksomheten.

Jeg har oppsummert min analyse av mine funn i figur 4, der jeg setter mine funn inn i Kotters trinnvise modell. Hensikten med figuren er å vise hvor det kan forventes at effekten av kategorien er mest synlig. Figuren viser også avhengighetsforhold mellom de ulike kategoriene, og i hvilken sekvens de bør fokuseres på for å få mest mulig ut av implementeringen av IMO resulosjoenen.

Figuren viser mine funn satt inn i Kotters modell for endringsledelse. Kotters ulike trinn ligger i toppen av figuren, mens de ulike kategoriene illustrers med piler. Pilenes lengde skal illustrere hvor effekten av kategorien først og fremst vil være synlig.



Figur 4

5.1 Kompetanse

Mine funn gir to tilnærminger til kompetanse innen maritim cybersikkerhet. Informanten fra Sjøfartsdirektoratet forteller at etaten og fagmiljøer er godt i gang med å tilby kurs til både rederi og mannskap innen fagområdet. Dette samsvarer med innholdet i Kotters trinn seks, fokus er å skape raske og synlige resultater.

Kompetansepilen har også en mindre tydelig forlengelse til Kotters trinn åtte, der fokus er å forankre endringene i bedriftskulturen og institusjonalisere de nye holdningene i virksomheten. Min forståelse for trinnet i konteksten av maritim cybersikkerhet, er at det er snakk om å skape varige endringer. Og i dette tilfelle varige endringer innen kompetanse og utdanning innen maritim cybersikkerhet. Mine funn tegner et bilde av at utdanning innen cybersikkerhet generelt, og spesielt innen maritim cybersikkerhet er mangelvare. Ingen av informantene kjente til målrettet utdanning, spisset kompetanse må etableres både som en del av den maritime fagutdanningen, og som en del av den tekniske utdanningen. Derfor forlenges kompetanse pilen til også å innebefatte permanente endringer, herunder en revisjon av maritimfagutdanning og maritim høyskoles fagplanen for også å favne om nødvendig cyberkompetanse.

5.2 Næringslivets forståelse for oppdraget

Mine funn indikerer at myndighetene på både politisk og strategisk nivå har gjennomført en vellykket informasjonskampanje(Meland, 2021) for å iverksette Kotters endringsreise. Temaet er blitt aktualisert og satt på dagsorden, godt hjulpet av jevnlige cyberangrep mot bransjen både nasjonalt og internasjonalt.

Kildene forteller om myndigheter som gradvis har endret fokus fra å drive opplysningsarbeid om standarden, til søkelys på kontroll av at kravene er implementert. Kontrollmyndighetene i Sjøfartsdirektoratet beskriver at inspektørene har tatt kontroll av IMOs cybersikkerhets krav inn i sine ISM inspeksjoner, og at de er i ferd med å ta i bruk pålegg om utbedring som sanksjoneringsform for avvik.

Jeg har satt denne kategorien inn i Kotters trinn fem, fordi myndighetene er i ferd med å gå over i en fase der de har fjernet hindringer. Det som til nå har vært en gullrot/pisk tilnærming

til maritim cybersikkerhet, går nå over i en fase der gulrota er spist opp og man står igjen med en pisk. Selve pisken vil være drivkraft i trinn seks, men basert på mine analyser av tema så er vi ikke på det trinnet riktig ennå.

5.3 Sektorielt ansvar

Mine funn forteller at fram til starten av 2023 var maritim cybersikkerhet noe som næringen håndterte selv, med unntak av større hendelser som iverksatte varslingsplikten med tanke på kriminelle handlinger. Men i 2023 fikk Kystverket oppdraget om å etablere et sektorielt responssenter for cybersikkerhet i maritim sektor. Denne beslutningen er tatt fra myndighetene.

Flere av mine informanter stiller spørsmål knyttet til hvorfor oppdraget om å etablere et responssenter ble gitt til Kystverket, fremfor at det ble etablert som et samvikesenter for de ulike bransjene i næringen. Samtidig som myndighetene stiller seg positiv til at næringen samles om et innslagspunkt for å ivareta bransjens behov for å overvåke den norske maritime cybersikkerheten.

Basert på mine funn har jeg plassert det sektorielle ansvaret på trinn seks i Kotters modell. Det gjør jeg fordi selv om myndighetene har brukt lang tid på å etablere et sektorielt responssenter, så er oppdraget gitt til en etat og iverksatt. Kotter beskriver i dette trinnet at det er viktig å skape og planlegge hurtige og synlige gevinster. Mine funn indikerer at etableringen ikke kan beskrives som hurtig i forhold til hva sektoren selv kan få til, men dog skal det sies at det offentlige normalt sett bruker lengre tid på å etablere nye organisasjoner.

Etableringen av responssenteret er i alle fall synlig for den maritime næringen, og viser at staten tar ansvar for å understøtte næringen med både informasjon og hjelp ved cyberangrep. Denne balansen mellom myndighetenes krav til næringen, og etablering av responssenter er viktig. Det tegner et blide av at myndighetene gjennom Kystverket og Sjøfartsdirektoratet tar sitt samfunnsansvar seriøst, og ønsker å bidra til en mer robust og resilient næring i form av sikring mot cyberangrep.

5.4 Videre implementering

Videre implementering betyr i min forskning - hva som ligger i fremtiden for maritim cybersikkerhet. Mine funn tegner et bilde av at IMOs cybersikkerhets resolusjon på mange

måter er starten på å skape en mer fartøysflåte som er meget resilient i forhold til digitale angrep. Innføringen av IMOs cyberkrav poengteres av flere kilder som viktig, men bør i fremtiden ikke bare differensiere på fartøyets størrelse og bruksområde. Det vil også være viktig å definere en teknologisk modenhet på fartøyene som reguleres av kravene, slik at man ikke skaper et behov for ivaretagelse av legacy systemer.

Basert på mine funn har jeg plassert den videre implementeringen på trinn åtte i Kotters modell. Trinnet særtegnes ved at det er snakk om varige endringer i både kultur og holdninger. Maritim cybersikkerhet er kommet på dagsordenen, og vi ser at nye cyberrelaterte krav kommer til fartøy som produseres. Intensjonen om å få cybersikkerhet inn som en driftsrutine har man lyktes med, samtidig som man ikke hviler på laurbærene. Med andre ord så er endringsreisen på mange måter fullført, samtidig som en ny endringsreise med nye og klarere definisjoner påbegynnes.

6 Analyse av funn sett opp mot faglitteratur

I dette kapittelet drøfter jeg de empiriske hovedfunnene opp mot oppgavens problemstilling og forskningsspørsmål. Kapittelet har fire underkapitler som figur 2 illustrerer. Hensikten med kapittelet er å belyse om oppgavens teori og empiriske funn kan fremstille mulige svar på oppgavens problemstilling.

Figur 5

Figur 5 skal vise hvordan de ulike kategoriene spiller inn mot forskningens problemstilling.

6.1 Kompetanse

Maritim næring er en næring med eldgamle tradisjoner i norsk sammenheng. Navigasjon og sjømannskap har prinsipielt ikke endret seg siden Leiv Eiriksson oppdaget Amerika, selv om verktøyene har endret seg.

Eksemplet fra vikingtiden kan dras videre, men budskapet er at fagplaner for både maritimfagskole og høyskole har samme kjernen av kunnskaps og ferdighetsmål. Fagplanene utvikles konservativt i forhold til samfunns og trusselutviklingen, og må oftest suppleres med spesialkurs for noen utvalgte få i besetningen enten det er teknisk eller operativ del av

besetningen (SDIR, 2020). I 2021 la regjeringen Solberg frem en nasjonal digital sikkerhetskompetanse melding (Justisdepartementet, 2021) der flere av tiltakene treffer maritim næring. Tiltak som Digital sikkerhet i yrkes- og profesjonsutdanninger eller Etter- og videreutdanning (EVU) innenfor IKT og digital sikkerhet understøtter en omforent oppfatning av at den digitale kompetansen må løftes i utdanningene til maritim sektor. Manglende inkludering av digital kompetanse og cybersikkerhet i fagutdanningene belyses også på nytt i NSMs Sikkerhetsfaglig råd - Et motstandsdyktig Norge der det påpekes et behov for å ha et nasjonalt løft for å ivareta nasjonens interesser (NSM, 2023).

Mine funn, fra samtlige kilder, erkjenner at tilgang til kompetent personell er krevende for den maritime næringen. Løsninger og konsekvenser av utfordringen materialiserer seg ulikt i de forskjellige nivåene. Hvert nivå beskriver løsninger som vil være relevant i ulike tidsaspekt, men som til sammen tegner et helhetlig bilde på kort, midlene og lang sikt.

Politisk nivå ser ingen quick fix på kompetanse utfordringen, og lener seg i større grad på at kompetansegapet ikke lar seg alene løse med endringer innen de maritime utdanningene. Informanten adresserer heller en løsning der mengden utdannet personell forblir den samme, men bruk av kunstig intelligens vil i større grad erstatte mennesket i deler av arbeidsprosessene. Noe som på sikt vil redusere kompetansegapet innen maritim cybersikkerhet.

På strategisk nivå beskriver informanten en annen fasett av kompetanseutfordringen. Her ser man at kompetansegapet skaper det som kalles «arbeidstakers marked». Der kompetente arbeidstakere er mangelvare og meget ettertraktet personell. De kan i større grad påvirke tilsettingsvilkår, og lett fristes av bedre vilkår hos nye arbeidsgivere med bedre vilkår. Mine funn indikerer at for kommunale og statlige virksomheter vil denne typen arbeidsliv tilby en hverdag der de ikke kan konkurrere med privat sektor med tanke på vilkår og lønn. Dermed rekrutteres det inn nye i staten, men når de har ervervet seg erfaring så drar de videre til privat sektor (Svendsen, 2020). Denne typen strømminger skaper utfordringer for å kunne etablere solide og erfarne fagmiljøer. Hvordan det offentlige skal kunne forsere disse utviklingene er vanskelig å predikere, da det offentlige ikke kan verken outsource eller endre lønnsvilkår for en hel næring uten en grundig prosess.

På operasjonelt nivå har man i større grad skoen på, og informanten forteller at den maritime næringen i liten grad har tid eller risikovilje til å vente på at det offentlige Norge skal ordne opp i utfordringen knyttet til tilgangen på kompetent personell innen maritim cybersikkerhet. Næringen oppfatter trusselen som troverdig, og konsekvensen av et angrep som eksistensiell. Av den grunn har de etablert NORMA Cyber som paraply organisasjon for maritim cybersikkerhet. Samtidig som stadig flere av rederiene outsourcer sine IKT tjenester til en tredjepart i andre land der tilgangen på kompetent personell er bedre, samt at lønnskostnaden er lavere. Denne løsningen løser problemet som næringen står i nå, men på lang sikt vil den kunne gi utforinger. Et eksempel på slike utfordringer er at virksomheter som outsourcer denne typen tjenester vil ha utfordringer i forbindelse med å kunne få oppdrag hos det offentlige Norge. Dette på grunn av at innholdet i stadig flere oppdrag omfatter tjenester regulert i Sikkerhetsloven. Noe som i neste runde vil stille krav til verdikjeder og sikkerhetsgodkjenning av leverandørens driftsrutiner og lokalisering av støtteressurser slik som IKT.

Det er ingen enkel løsning på kompetanseutfordringen knyttet til det digitale domenet. Det brukes ord som krise, dugnad og kompetanseløft for å aktualisere utforingene. Uavhengig av hvilket nivå som skal løse utfordringene, er det tydelig at alarmhåndteringen er vanskelig å få på agendaen. Digitale angrep på Norge har ennå ikke resultert i uopprettelig skade og/eller tap av liv, og når derfor i liten grad opp i prioriteringslista til myndighetene(NSM, 2023). Uten at cybersikkerhet kommer høyere opp på agendaen, vil både nasjonen og næringen være sårbar.

6.2 Næringslivets forståelse for oppdraget

Store norske leksikon beskriver at «å forstå» er å begripe, fatte, gjøre bruk av forstanden, innse eller oppfatte noe. Denne romslige definisjonen gir kategorien et innhold, ikke entydig svar. Forståelse i seg selv er dog heller knytta i større grad til persepsjon, selv om man i det fleste tilfeller håper at persepsjonen etterfølges av en forventet handling. Fortrinnsvis for å kunne løse et problem eller dilemma.

Mine funn indikerer at næringslivets forståelse for oppdraget er god. Mine informanter tegner et bilde av en meget oppgående næring, som har god forståelse for utfordringer næringen står ovenfor i god tid før det presenteres som et krav fra myndighetene. På den ene siden sier

informanten på operasjonelt nivå at «de ulike rederiene i bransjen preges av hvor hoveddelen av deres oppdrag gjennomføres, fortrinnsvis innenriks, utenriks eller konfliktområder. Noe som gjenspeiler seg i rederiets fokus og prioriteringer.» På den andre siden sier informanten på politisk nivå sier at «sjøfartsnæringen er meget kommersiell, og har alltid vært kjennetegnet av at de er meget gode på å snu på kronen.» De to utsagnene tegner et mer nyansert bilde av næringens forståelse av oppdrag.

Informanten fra Sjøfartsdirektoratet forteller om informasjonskampanjer rettet mot alle deler av næringen, som en del av implementeringen av IMOs cybersikkerhetsresolusjon. Selv om informasjonskampanjene knyttet til innføringen av myndighetskravene, har maritim cybersikkerhet gradvis tatt en økt del av nyhetsbilde siden 2010. Deretter har ulike statlige utredninger belyst sårbarheten til maritim næring i knyttet til cybersikkerhet.

Funnene indikerer som nevnt at oppdraget, trusselen og konsekvensen av digitale angrep mot fartøy eller rederi er godt forstått i næringen som helhet. De har god forståelse for å skape profitt, og sitter ikke på gjerdet og venter på at verden skal komme til dem. Ei snarere tvert imot. Ifølge Sjøfartsdirektoratet er gulroten fra myndighetene i for bindelse med implementeringen i stor grad spist opp. Noe som blir tydelig når vi ser at avvik blir påpekt, og pålegg om utbedring blir overlevert til fartøyer. En utvikling som manifesterer at implementeringen har passert Kotters fire første trinn, og er godt i gang med å klatre de resterende fire trinnene.

Informanten i Sjøfartsdirektoratet forteller at tilsyn av IMO-cybersikkerhetsresolusjon er innlemmet som en del av ISM-inspeksjonen som gjennomføres på fartøyer over 500 bruttotonn og/eller som har 100 passasjerer eller flere(SDIR, 2014). ISM inspeksjonen gjennomføres per femte år, men som med et mellomliggende tilsyn per 2,5 år. Det kan i verste fall medføre at et fartøy kan unngå å iverksette kravene i løpet av fem år, spesielt om pisken ikke svinges for hardt når avvik blir detektert ved mellomliggende tilsyn. En slik prokrastinering er ikke formålstjenlig, men er det høye kostnader forbundet med å implementere en god nok digitalsikring av fartøyet så kan det være den beste kursen å seile.

I intervjuet med informanten på operasjonelt nivå tok jeg opp problemstillingen knyttet til prokrastinering av tilsyn, for å utsette kostnadene som er forbundet med å iverksette kravene.

Han sa at han opplevde det mer som et avvik, enn normalen i næringen. Han poengterte at IMOs cybersikkerhetsresolusjon stiller krav til både rederiet og fartøyene vedrørende deres tekniske og prosedurale evne til å håndtere digitale angrep. Rederiene implementerer derfor oftest kravene for rederiet som helhet, med sine fartøyer. Derfor blir det vanskelig å implementere en fragmentert digital sikring av rederiet.

Gjennom mine intervjuer tegner det seg et helhetlig bilde av at Sjøfartsdirektoratet som kontrolletat har lykkes i det som professor Kotter kaller «å etablere en nødvendighet» for implementeringen av kravene. Store delen av flåten som reguleres av kravene vil i løpet av 2023 operere i samsvar med myndighetskravene, mye på grunn av godt forarbeid fra myndighetene og bransjen som helhet.

6.3 Sektorielt ansvar

Etter hvert som jeg har intervjuet kilder både innen det maritime domenet og cybersikkerhetsdomenet, så fremstår fortsatt det sektorielle ansvaret som litt uavklart. Det er besluttet at Kystverket skal etablere et sektorielt responssenter, som skal ivareta den maritime næringens behov knyttet til cybersikkerhet. Rolle, ansvar og myndighet knyttet til senteret var det dog ingen av informantene som kunne fortelle. Fraværet av kunnskap om responssenteret skyldes ikke gradering, men heller at de ikke kjente til det. NSM har tydelige beskrivelser av rammer – ansvar – myndighet innen på sine websider(NSM, 2018a). Gapet mellom de ulike nivåene med tanke på hvem gjør hva er urovekkende, men vil trolig bli fanget opp når SRM blir operativ i løpet av 2023.

Mine funn underbygger epistelen om veien til denne masteroppgaven. Informanten kunne fortelle at det ved årsskifte 2022/23 ble besluttet at det sektorielle responssenteret skulle opprettes i og driftes av Kystverket. Dermed ble det sektorielle ansvaret for cybersikkerhet lagt til en av flere etater som har rollen som kontrollmyndighet i den maritime sektoren. Informanten som har vært involvert i utredningen stilte seg undrende til denne løsningen, da den ikke gav noen oppgaver til Sjøfartsdirektoratet.

Jeg deler på mange måter oppfatningen til informanten fra Sjøfartsdirektoratet. I andre lignende tilfeller har staten valgt å etablere samvirkesenter for koordinering og

informasjonsutveksling. Et godt eksempel på dette er Felles cyber koordinerings senter (FCKS) der NSM, Kripos, PST og Etterretningstjenesten samarbeider og utveksler informasjon fra sine respektive kanaler. Tar vi eksemplet fra Etterretning og sikkerhetstjenestene (EoS), er det et komplekst domene å drive forebyggende og risikoreduserende trussel håndtering. Overfører vi rasjonale til den maritime sektoren så krever den samhandling fra blant annet Sjøfartsdirektoratet, Kystverket, Fiskeridirektoratet og Petroleumstilsynet. En sektor med mange nisjenæringer som krever inngående detalj kunnskap. I den sammenheng har jeg ingen funn som understøtter en etablering av sektorielt responssenter i en av etatene, fremfor å etablere et felles samhandlingssenter på lik linje med FCKS(Bakke, 2022).

Informanten på operasjonelt nivå presenterte noen fasetter av problemsstillingen som ikke fanges opp gjennom prinsipielle diskusjoner. Han kunne fortelle at selv om det opprettes et sektorielt responssenter for den maritime næringen, så vil de bare støtte cyberangrep på norske fartøy som blir angrepet i norske farvann. Norske nasjonale kontrollmyndigheter har ikke myndighet til å håndtere hendelse som skjer i andre farvann, og hendelser må understøttes av de nasjoner som farvannet tilhører. Ifølge SSB utgjør NIS registrerte fartøy om lag 40 prosent av den norske handelsflåten, noe som gjør at rederiene i stor grad er avhengig av egen evne eller paraplyorganisasjoner i forbindelse med hendelses håndtering av ulike cyberangrep(SSB, 2023).

På politisk og strategisk nivå tar informantene opp at man på lengre sikt må vurdere nye måter å organisere det digitale forsvaret. Dette er også tema som både i Utsyns fagnotat om cybersikkerhet der de anbefaler etableringen av en felles digital grunnmur som skal etablere et godt fundament og ivareta samhandling mellom etater og sektorer(Bakke, 2022). NSMs sikkerhetsfaglige råd adresserer også utfordringer knyttet til uklare ansvarsforhold knyttet til håndtering av tverrsektorielle sikkerhetstruende hendelser(NSM, 2023). Basert på mine funn, er jeg enig i at Norge må revurdere hvordan den digitale sikkerheten skal løses. Selv om det i dag er et bærende prinsipp at digital sikkerhet er den enkelte bedrifts eget ansvar. Det vil i mange tilfeller være tiltak av en defensiv art, men at bedriften i større grad er avhengig av støtte fra offentlige myndigheter ved et angrep. I den sammenheng hviler det et ansvar på

myndighetene å yte denne støtten til sine innbyggere, og i så måte burde man se på mulige løsninger for å organisere en slik støtte. Bærende prinsipp for en slik omorganisering kan være å etablere robuste fagmiljøer og bortfall av siloer slik at kompetent fagpersonell enkelt kan omrokeres for å effektiv håndtere hendelser.

Sektorprinsippet og etatsvise responssenter er en særnorsk problemløsningsmodell som er moden for revisjon (Riksrevisjonen, 2022). I noen tilfeller er det en optimal organiseringsform for hendelseshåndtering, men når det kommer til cybersikkerhet så er jeg usikker på hvor gunstig det er for både næringen. Organiseringsformen innebærer mange rapporteringsledd som primært kan motta situasjonsoppdateringer, men dog i liten grad kan yte noen støtte til de berørte partene.

6.4 Veien videre

I denne forskningskategorien som omtales som «Veien videre», har jeg knyttes den opp mot Kotters trinn åtte, som innebefatter å institusjonalisere de nye holdningene eller med andre ord å skape varige endringer. Mine informanter predikerer ulike momenter som de tror vil påvirke veien videre, og på mange måter kan man si at momentene som belyses i veien videre vil danne starten på nye endringsreiser. Og på den måten vil maritim cybersikkerhet være et prosjekt bestående av mindre prosjekter som alltid vil ha som mål å utvikle næringens cybersikkerhet.

Mine funn knyttet til det politiske nivået beskriver en fremtid der flere av arbeidsprosessene som i dag driftes av mennesker vil bli erstattet av kunstig intelligens. Noe som allerede bekreftes fra operasjonelt nivå, der kunstig intelligens ikke bare detekterer uønsket nettverksaktivitet, men også leser ut og sorterer systemalarmer. Automatiseringen vil i stadig større grad være med på å øke effektiviteten til defensive cybersystemer. Man bør i m Man bør i den sammenheng også trekke frem at en angriper også vil bruke de samme ressursene for å kunne nå sine mål med sitt digitale angrep.

Informanten fra NSM forteller at stadig nye regelverk er i ferd med å tre i kraft, enten det er NIS2 (Europa, 2023) reglementet eller en oppdatert sikkerhetslov. Verktøyene myndighetene har til disposisjon blir stadig bedre, samtidig som samhandlingen mellom påtalemyndighetene

både innad i EU og internasjonalt muliggjør påtale og straffeforfølgelse utenfor Norges grenser.

På det utøvende nivået tegnes det et bilde av at IMOs cybersikkerhetskrav for maritim næring på mange måter har dannet en startlinje for hele næringen. Selv om kravene kan tolkes ulikt blant IMOs medlemsnasjoner, gir den på mange måter et omforent utgangspunkt for å bygge videre på. Informanten på operasjonelt nivå forteller at de neste årene vil det komme nye og skjerpede krav til nye fartøy, og med skjerpede krav til autonome fartøy. Etter min mening er dette en bra vurdering. Nye fartøy er mer teknisk avansert og automatisert. Et angrep på nyere fartøy vil ha større angrepsflater, samt større spredningspotensiale. Mens eldre fartøy er mer primitive, men har samtidig flere manuelle overstyringsmetoder som vil kunne redusere konsekvensen av et digitalt angrep. Til slutt må det trekkes frem at fremtidens autonome fartøyer vil være designet med tanke på cybersikkerhet og resiliente fartøyer.

Veien videre vil gi en bedre sikret fartøysflåte, samt en rederiorganisasjon som i større grad har beredskapsplaner og teknisk bemanning for å kunne håndtere slike angrep. Den globale maritime næringen har fått seg et løft innen egensikring, og vil i fremtiden være mer resilient mot digitale angrep. Selv om det nå foregår et skippertak for å få maritim næring opp på et akseptabelt nivå innen cybersikkerhet, må veien videre være preget av et kontinuerlig forbedringsarbeid for å ha best mulig digitalt forsvar av næringen.

6.5 Relaterte arbeid

Jeg har som en del av min forskningsprosess kommet over annen forskning som til dels har hatt overlappende fokus med min problemstilling og forskningsspørsmål. Sjøfartsdirektoratet har ledet et arbeid for å utvikle en strategi for cybersikkerhet i maritim sektor. Den bygger primært på en trusselvurdering levert av SINTEF (Meland, 2021) og en ROS analyse for maritim digital sikkerhet (DNV-GL, 2020), disse produktene var med på å danne utgangspunktet for Sjøfartsdirektoratets strategi for maritim digital sikkerhet(SDIR, 2020).

Trusselvurderingen fra SINTEF(Meland, 2021) gir et bredt og overordnet bilde av den siste tidens hendelser som har berørt den maritime sektoren. De utleder først og fremst hvilke angrepsflater som har vært brukt, og hvilke angrepsmetoder man har detektert. Dette bakteppet gir en god forståelse for hva den maritime næringen kan komme til å stå ovenfor,

og tallfester i stor grad at vi det vi ser mest av er det som er vurdert som fiendens mest sannsynlige handlemåte. Mens angrepene som vi frykter mest, også kjent som fiendens farligste handlemåte er noe som man i liten grad finner i angrepshistorikken for cyberangrep på verdensbasis. Det bør i den sammenheng poengteres at konsekvensene av det som kalles «fiendens farligste handlemåte», som i maritim kontekst er angrep på OT systemer om bord på fartøy regnes også som det mest farlige typen av angrep.

Det Norske Veritas (DNV) har med bakgrunn i oppdraget fra Sjøfartsdirektoratet utviklet en Risiko og Sårbarhetsanalyse (ROS)(DNV-GL, 2020) for maritim cybersikkerhet i Norge. De har gjennomført en kvantitativ spørreundersøkelse blant rederi, fartøy og mannskaper i næringen. Konklusjonen til DNV var at regelverk for maritim digital sikkerhet bør være i samsvar med internasjonale lover og regler. Sjøfartsdirektoratet bør tilby veiledning innen de viktige områdene for IKT. Samt at industrien trenger også støtte til å utvikle og introdusere passende tekniske IKT sikkerhetstiltak. Spørreundersøkelsen hadde god oppslutning og gir en pekepinn på hvilke behov næringen har fra det offentlige, samt hvilke holdningen de har til en strengere regulering av den maritime digitale sikkerheten.

Arbeidet til SINTEF og DNV var viktige innspill til Sjøfartsdirektoratets rapport «Overordnet strategi for maritim digital sikkerhet»(SDIR, 2020). Rapporten er omfattende med gode anbefalinger fra et etatsperspektiv, der det anbefaler blant annet å etablere et sektorielt responsmiljø (SRM) og tiltak knyttet til kompetansebygging innen digital sikkerhet i den maritime næringen. Rapporten går mer i dybden på hvordan tiltakene bør implementeres, og understøtter i stor grad mine funn.

Etablering av SRM anbefales, og tjenestene de tilbyr til næringen er godt beskrevet i rapporten. Rolle, ansvar og myndighet er til dels godt beskrevet, men i og med at næringen organiseres under flere departement, vil særlig myndighetsaspektet og samvirkedimensjonen bli mer tydelig etter hvert.

Strategien tar også frem kompetansebygging som tre av tiltakene, herunder digital sikkerhetskompetanse, sikkerhetskompetanse i internasjonalt regelverk og opplæringstiltak. Tiltakene samsvarer meget godt med mine funn og analyser, og understøtter næringens behov for at det gjennomføres en revisjon av de formelle maritime utdanningene for å skape en

langsiktig gevinst. Og at det samtidig utvikles kurs og annen opplæring av kortere varighet for å oppdatere allerede utdannende sjøfolk.

Annen forskning og strategier har benyttet andre metoder for å samle inn metadata til å underbygge deres funn. Min forskning og ovenfor nevnte forskning har metodisk lite overlapp, men begge har til dels store overlappende funn. Den ulike vinklingen på samme tema, er slik sett med på å stadfeste mine funn selv om mine funn til slutt anvendes i en annen kontekst.

6.6 Oppsummering

Mine funn og analyser tegner et bilde av en næring i godt driv framover for å møte myndighetenes krav om digitalsikkerhet. Næringen er i stor grad i inngripen med kategoriene «Næringslivets forståelse for oppdraget» og «Veien videre». De to kategoriene representer ulike faser i Kotters modell, men min forståelse er at næringen i høy grad oppfyller sin rolle som en seriøs portvokter for maritim cybersikkerhet.

Kategoriene «Kompetanse» og «Sektorielt ansvar» knyttes sterkere opp til myndighetene. Min forskning underbygger at disse oppgavene i liten grad er påbegynt. Ser man dette opp mot Meld St nr 10(Regjeringen, 2016) fra 2016 så adresseres viktigheten av både etablering av sektorielle responsmiljøer, og en revidering av undervisningsprogram for å øke fokuset på digital sikkerhet. I 2023 viser forskningen at det er lite bevegelse innen disse to temaene. Deltema har vært utredet, og i 2023 er beslutningen om å etablere et sektorielt responssenter for maritim næring besluttet. Men det har gått sju år siden Stortingsmeldingen påpekte behovet, og trusselbildet og mengden angrep på norsk maritim næring har økt jevnt.

Forskningen i denne oppgaven tegner et bilde av at fokuset som har vært på at den maritime næringen skal iverksette IMO cyberresolusjonen i samsvar med fremdriftsplanen til myndighetene, så har myndighetene ikke løst sitt oppdrag om å skape langsiktige gode rammer for kompetansebygging innen maritim cybersikkerhet. I den sammenheng er samspillet mellom stat og næring viktig for å kunne ha rett kompetanse til de som står i fremste linje, hver dag.

Generaliserer vi mine funn til å fokusere på de fire kategoriene, så er min oppfatning at de kategoriene som myndighetene har rollen som pådrivere eller endringsagenter de som ikke kommer til skudd i forbindelse med implementeringen av IMO resolusjonen. Min forskning har som formål å analysere mine funn i konteksten av Kotters trinn fem til og med åtte. Men når det kommer til «kompetanse» og «sektorielt ansvar» viser mine analyser at slett arbeid innen endringsledelse i Kotters modell trinn en til og med fire, gjør konkretisering av oppgaver og fremgang i de kategoriene utfordrende.

Hvorfor er det utfordrende for myndighetene å gjennomføre de oppgavene som knyttes til de kategoriene som de har ansvar for. Jeg støtter meg i stor grad på Meld St 10(Regjeringen, 2016) der det poengteres at utvikling av sektorielle responssenter er utfordrende. Blant annet på grunn av at flere departement skal delta i finansieringen av aktiviteten, samt at er liten tilgang på kompetent personell i de enkelte departementene. I en Kottersk kontekst vil det si at de ikke lykkes med å skape en følelse av nødvendighet eller sette sammen en kapabel endringskoalisjon, som samsvarer med trinn en og to i modellen. Endringsledelse krever at trinnene i modellen følges kronologisk, og endringsreisen vil bli ineffektiv om de hoppes over.

Kategorien kompetanse har mange likheter i forhold til grunnleggende utfordringer og avklaring med kategorien «sektorielt ansvar». I Sjøfartsdirektoratets strategi for maritimcybersikkerhet(SDIR, 2020) belyses dette i deres tiltaksliste ved at «Kystverket og Sjøfartsdirektoratet, tydeliggjør sine behov ovenfor utdanningsmyndighetene, spesielt knyttet til sin egenart på digital sikkerhetskompetanse». Delingen av kompetanseutviklingen som domene mellom maritim sektor og utdanningsmyndigheten gjør at endring og omstilling av fagutdanninger og fagplaner gjøres som delaktiviteter i et større revisjonsarbeid, istedenfor som en mindre prosess der maritimsektors behov er hovedfokus. Slike byråkratiske hindringer påvirker framdriftens tempo negativt, mens den digitale motstanderen på sin side øker sin evne til å bli stadig mer avansert.

7 Konklusjon

I konklusjonskapittelet vil jeg prøve å fremheve mine viktigste funn som fremgår fra diskusjonskapittelet. Formålet er å besvare mitt problemformulering:

Hvilken endringsreise skaper innføring av IMO MSC.428(98) innen norsk maritim næring, og hvilke erfaringer knyttes til den?

Min forskning viser til en innføring av cybersikkerhetskrav som er godt underveis i den maritime næringen, mens myndighetens totale tilnærming framstår som noe fragmentert. Mine funn indikerer at myndighetene i stor grad har hatt fokus på å iverksette kravene i næringen, for deretter å omstille egne leveranser som understøtter næringens behov. Det er slik sett lite av Kotters endringsledelse å spore fra myndigheten internt, men dog kan jeg identifisere trinnene i myndighetenes endringsstyring opp mot den maritime næringen.

Funnene tegner et bilde av en næring som tar cybersikkerhet på alvor, men som er tvunget til å prioritere mellom etterlevelse av krav fra myndighetene og lønnsomhet. Myndighetene har implementert IMO-cybersikkerhetskrav som en del av rederienes og fartøyenes ISM kode, og er på vei til å håndheve disse kravene. Innen kort tid vil samtlige fartøy og rederi være kontrollert, og godkjent eller ha mottatt pålegg om utbedring. Alle parter er slik innforstått med hvilke krav som stille. Det er med andre ord bare en vei for maritim cybersikkerhet, og det er framover.

På den andre siden viser mine funn at det fortsatt er store hull som må tettes for at endringen skal være bærekraftige, samt skape resiliens innen cybersikkerhet i den maritime næringen. Fra samtlige informanter adresseres behovet for økt fokus på kompetanse og etablering av sektorielle statlige ressurser som næringen kan støtte seg på.

Kompetanse skaper langsiktige gode løsninger, og digital sikkerhetskompetanse nevnes i stadig flere sammenhenger. Det er på tide å revidere fagplaner ved både fagskole og høyskole for maritim utdanning, slik at sjømannskaper må bruke lang tid på ekstra utdanning etter gjennomført maritim utdanning. Den beste plassen for utdanning er først og fremst på skoler, og ikke på kurssenter som en del av en friperiode i turnusen på havet.

Sektorielt responssenter belyses i ulike fasetter når jeg har jobbet med informanter og sekundærlitteratur. Strategien fra Sjøfartsdirektoratet beskriver både rolle, ansvar og myndighet, men mine funn indikerer at selv om beslutningen om etablering er fattet er det

ennå en del løse tråder i forhold til hvordan det sektorielle responssenteret skal operere og hvilken kapasitet de egentlig har.

Jeg vil til slutt si at endingsreisen knyttet til innføring av IMOs cybersikkerhetsresolusjon har vært en nødvendighet. Det har satt en ulmende brann på agendaen. Selv om endringsreisen knyttet til innføringen av IMOs cybersikkerhetskrav til slutt vil komme i havn, vil den bli avløst av nye nasjonale og internasjonale krav som skal ivareta næringens digitale motstandskraft.

I et beredskapsperspektiv er innføringen av IMOs cybersikkerhetskrav helt nødvendig for å unngå at Norges maritime næring skal bli sortert som lavt hengende frukt for fremmende makter og kriminelle aktører. En solid digital grunnmur med adekvate sikringstiltak gjør at den maritime næringen ikke fremstår som et lett bytte, og de angrep på norske interesser blir derfor mer krevende. Om vi lykkes måles ikke i antall angrep som vi blir utsatt for, men dog heller antallet angrep som vi har slått tilbake.

8 Referanseliste

Bakke, S. (2022). STRATEGISK CYBERSIKKERHET- 6 F O R S L A G F O R M E R RO B U S T D I G I T A L S I K K E R H E T. *Prosjekt utsyn*. Retrieved from https://www.prosjektutsyn.no/wp-content/uploads/2021/06/Fagnotat-cybersikkerhet.pdf

BIMCO. (2020). THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS. In. BIMCO.

Cisco. (2022). How Do OT and IT Differ? Retrieved from https://www.cisco.com/c/en/us/solutions/internet-of-things/what-is-ot-vs-it.html

DNV-GL. (2020). *ROS analyse for maritim digital sikkerhet*. Retrieved from https://www.sdir.no/contentassets/174739a55adb44098b05bcb8ef3b2f65/dnv-gl---2020-09-15-ros-analyse-for-maritim-digital-sikkerhet-v1---report.pdf

Europa, P. (2023). *The NIS2 Directive: A high common level of cybersecurity in the EU*. Retrieved from https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

Executive, T. m. (2020). Vard Hit by Cyberattack. Retrieved from https://maritime-executive.com/article/vard-hit-by-cyberattack

Fangen, K. (2015). Kvalitativ metode. Retrieved from https://www.forskningsetikk.no/ressurser/fbib/metoder/kvalitativ-metode/

IMO. (2017). *MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS*. UN Retrieved from https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

ISO. (2023). ISO/IEC 27001 - Information security management systems. Retrieved from https://www.iso.org/standard/27001

Johannesen, C. T. (2021). *Forskningsmetode for økonomiske og adminstrative fag*: Abstrakt forlag.

Justisdepartementet. (2021). *Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet*. Regjeringen Retrieved from https://www.regjeringen.no/contentassets/d256b455415c4cae8a710f62cc97d4f9/no/pdfs/stm202220230009000dddpdfs.pdf

Kavallieratos, G. (2022). *Critical Infrastricture Protection.* Paper presented at the NTNU Cybersecurity, Gjøvik.

Kotter, J. (1995). *Leading change: Why transformations efforts fail*: Harvard Business Rewiev.

Kotter, J. (Producer). (2012). What is the difference between change management and change leadership.

Lysne. (2015). *Digital sårbarhet –*

sikkert samfunn. OSLO

Mattord, M. E. W. H. J. (2020). *Principles of Information Security* (Vol. 11). Kennesaw State University: CENGAGE.

Meland, P. H., Karin Bernsmed, Ørnulf Jan Rødseth, Dag Atle Nesheim. (2021). *Trusselvurdering i forbindelse med strategi*

for maritim digital sikkerhet. Retrieved from Trondheim: https://www.sdir.no/contentassets/174739a55adb44098b05bcb8ef3b2f65/trusselvurdering-i-forbindelse-med-strategi-for-maritim-digital-sikkerhet.pdf?t=1610910211600

Nations, U. (2021). Den internasjonale sjøfartsorganisasjonen (IMO). Retrieved from https://www.fn.no/om-fn/fns-organisasjoner-fond-og-programmer/den-internasjonale-sjoefartsorganisasjonen-imo

NIST. (2023a). Computer Security Resource Center. Retrieved from https://csrc.nist.gov/

NIST. (2023b). Cybersecurity. Retrieved from https://www.nist.gov/cybersecurity

NSM. (2018a). *Rammeverk for håndtering av IKT-hendelser*. NSM Retrieved from https://nsm.no/regelverk-og-hjelp/andre-publikasjoner/rammeverk-for-handtering-av-ikt-hendelser/

NSM. (2018b). *VEDLEGG 4 – RAMMEVERK FOR HÅNDTERING AV IKT-SIKKERHETSHENDELSER*. NSM Retrieved from https://nsm.no/getfile.php/133863-1593022742/NSM/Filer/Dokumenter/vedlegg-4---begrepsliste.pdf

NSM. (2020). Kvalitetsordning for leverandører som håndterer IKT-hendelser. Retrieved from https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/kvalitetsordning-for-leverandorer-som-handterer-ikt-hendelser

NSM. (2023). *Sikkerhetsfaglig råd - Et motstandsdyktig Norge*. Retrieved from https://nsm.no/getfile.php/1312994-1683615611/NSM/Filer/Dokumenter/Rapporter/Sikkerhetsfaglig%20r%C3%A5d%20-%20Et%20motstandsdyktig%20Norge.pdf

Regjeringen. (2016). *Meld. St. 10 (2016–2017) Risiko i et trygt samfunn — Samfunnssikkerhet*. Retrieved from https://www.regjeringen.no/no/dokumenter/meld.-st.-10-20162017/id2523238/

Riksrevisjonen. (2022). *Myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor*. Retrieved from https://www.riksrevisjonen.no/globalassets/rapporter/NO-2022-2023/myndighetenes-samordning-av-arbeidet-med-digital-sikkerhet-i-sivil-sektor.pdf

Ritchie, R. (2019). Maersk: Springing back from a catastrophic cyber-attack. *Global Intelligence for digital leaders*. Retrieved from https://www.i-cio.com/management/insight/item/maersk-springing-back-from-a-catastrophic-cyber-attack

SDIR. (1978). STCW - Den internasjonale konvensjon om normer for opplæring, sertifikater og vakthold for sjøfolk, 1978, med endringer. Retrieved from https://www.sdir.no/sjofart/regelverk/internasjonale-konvensjoner/stcw/

Forskrift om sikkerhetsstyringssystem for norske skipForskrift om sikkerhetsstyringssystem for norske skip og flyttbare innretninger, (2014).

SDIR. (2020). Overordnet strategi for https://www.sdir.no/contentassets/174739a55adb44098b05bcb8ef3b2f65/2020-12-18---rapport-overordnet-strategi-for-maritim-digital-sikkerhet---v3-klar-til-levering-nfd-og-sd.pdf?t=1684316989315maritim digital sikkerhet.

Lov om nasjonal sikkerhet (sikkerhetsloven, (2019).

Silverman, D. (2006). *Interpreting qualitative data: Methods for analyzing talk, text and interaction*. Los Angeles: Sage.

Solms, R. v. (2013). From information security to cyber security. *Computer & Security, 38*, 97-102. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0167404813000801#preview-section-snippetsRossouw von Solms

SSB. (2023). Handelsflåten, norskregistrerte skip. Retrieved from https://www.ssb.no/transport-og-reiseliv/sjotransport/statistikk/handelsflaten-norskregistrerte-skip. https://www.ssb.no/transport-og-reiseliv/sjotransport/statistikk/handelsflaten-norskregistrerte-skip

Svendsen, B. (2020). *Økt evne til å kombinere menneske og teknologi*. Retrieved from https://www.regjeringen.no/contentassets/374492dfae2f41a18f9b01e8678b468a/svendsen-utvalget--okt-evne-til-a-kombinere-menneske-og-teknologi.pdf

Vold, L. B. (2023). *Norma Cybe Annual Threat Assesment*. Retrieved from

Vedlegg 1: Intervjuguide

Intervjuguide

Navn:

Alder:

Stilling:

Antall år i stilling:

Antall år i bransjen(sikkerhet):

Hvilke bedriften har du jobbet med sikkerhet i:

Utdanning:

Hvor lenge har du jobbet med cybersikkerhet? Og cybersikkerhet knyttet til maritim næring?

Hva er din kjennskap til IMO's Cybersikkerhetsstandard som ble innført i 2020?

Hvordan opplever du maritim cybersikkerhet? Er det en bunndreven eller ledelsedreven utvikling.

Hvordan vurderer du effekten av innføringen av IMO standarden i Norge

I hvilken grad følger politisk nivå opp fremdriften av innføringen av cyberkravene?

Hvordan rapportes fremdriften i næringen?

Etter at IMO standarden ble innført så har det vært regjeringsskifte. Påvirker det fremdriften/fokus i implementeringen?

Opplever du en utvikling i cybersikkerhetsfokus i maritim næring etter innføring av IMO standarden/2020?

Tror du det kommer av IMO standarden? Eller andre årsaker.

Er det snakk om et kulturskifte?

Hvordan bør man fortsette utviklingen? Incentiver?

Hvordan vurderer du implementeringen av IMO standarden?

Hva kunne blitt gjort annerledes

Er det noe annet du vil ta opp?

Vedlegg 2: Samtykkeskjema

Vil du delta i forskningsprosjektet

"Cybersikkerhet i maritim næring i lyset av innføringen av IMOs cyberresolusjon"

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å kartlegge erfaringene ved innføring av IMOs krav til maritim cybersikkerhet. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål
Formålet med mitt forskningsprosjekt er å kartlegge erfaringene knyttet til innføring av IMOs krav vedrørende innføring krav til maritim cybersikkerhet.
Jeg vil gjennom disse undersøkelsene prøve å høste erfaringene fra ulike nivåer innen etater, rederier og fartøy, og prøve å se de innsamlede dataene i en organisasjonsutvikling kontekst. Jeg gjør dette som en del av min masteroppgave innen Beredskap og sikkerhetsledelse ved Nord Universitet.
Hvem er ansvarlig for forskningsprosjektet?
Handelshøyskolen ved Nord Universitet er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?
Jeg ønsker å intervjue deg om din erfaring med innføringen av IMOs krav til cybersikkerhet i maritim næring. Du blir spurt om å være informant på grunn av din stilling eller rolle knyttet til innføring av denne standarden i din organisasjon. Du er en av ti personer som er blitt forespurt om delta i denne undersøkelsen.

Hva innebærer det for deg å delta?
Jeg ønsker å samle inn erfaringer knyttet til IMO standarden innen cybersikkerhet i maritim næring ved hjelp av kvalitativ metode. Det gjør jeg gjennom intervju med et utvalg av informanter, deriblant deg. Av praktiske årsaker ønsker jeg å gjennomføre intervju over TEAMS, for å kunne enkelt bearbeide data i etterkant. Intervjuet blir gjennomført ved hjelp av Nord Universitet sin TEAMs lisens, og opptaksdata vil bli lagret på NORD UNIVERITET sine servere.

Hvis du deltar i dette forskningsprosjektet så innebærer det et intervju på om lag 45 minutter.

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det

vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

Dine personopplysninger vil bare være tilgjengelig for meg som behandlingsansvarlig og min veileder. Opplysningene vil bli lagret på et beskyttet filområde ved Nord Universitets server, og tilgang styres gjennom digitale sikringstiltak. Informasjonen vil bli anonymisert gjennom personinformasjon om informanten oppbevares på et annet sted, og kan ikke knyttes til de innsamlede data.
Det er ikke noe mål at informanten skal kunne identifiseres ved publikasjon av forskningsoppgaven.

Hva skjer med personopplysningene dine når forskningsprosjektet avsluttes?
Prosjektet vil etter planen avsluttes 1.juli 2023. Etter prosjektslutt vil datamaterialet med dine personopplysninger anonymiseres. Det vil gjøres gjennom at video opptak slettes, og den godkjente transkripsjonen tas vare på videre. Etter 1.1.2023 vil deretter transkripsjonen av data også slettes.

Hva gir oss rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra *Nord Universitet* har Personverntjenester vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:

- Nord Universitet ved Mass Soldal Lund, tlf 47978466.
- Vårt personvernombud: Toril Iren Kringen, tlf 74 02 27 50.

Hvis du har spørsmål knyttet til Personverntjenester sin vurdering av prosjektet, kan du ta kontakt med:

- Personverntjenester på epost (personverntjenester@sikt.no) eller på telefon: 53 21 15 00.

Med vennlig hilsen

Prosjektansvarlig
Mass Soldal Lund
(Forsker/veileder)

Eventuelt student
Ole Andreas Lereim

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *[sett inn tittel]*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ å delta i *intervju*
- ☐ *at opplysninger om meg publiseres slik at jeg kan gjenkjennes i artikler*

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

---

(Signert av prosjektdeltaker, dato)