Bacheloroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for ingeniørvitenskap
Institutt for havromsoperasjoner og byggteknikk

Magnus Gjerde, Andreas Sørum og Andreas Mulelid Kvam

# Digitalisering knyttet til sikker drift og cybersikkerhet på fartøy

## Hvordan opplever den maritime næringen at digitalisering påvirker sikker drift og cybersikkerhet på fartøy?

Bacheloroppgave i Nautikk
Veileder: Marie Haugli Larsen
Juni 2022

NTNU
Kunnskap for en bedre verden

Magnus Gjerde, Andreas Sørum og Andreas Mulelid Kvam

# Digitalisering knyttet til sikker drift og cybersikkerhet på fartøy

## Hvordan opplever den maritime næringen at digitalisering påvirker sikker drift og cybersikkerhet på fartøy?

Bacheloroppgave i Nautikk
Veileder: Marie Haugli Larsen
Juni 2022

Norges teknisk-naturvitenskapelige universitet
Fakultet for ingeniørvitenskap
Institutt for havromsoperasjoner og byggteknikk

NTNU
Kunnskap for en bedre verden

# FORORD

Denne bacheloroppgaven er det avsluttende arbeidet for tre bachelorstudenter på studieprogrammet nautikk ved institutt for havromsoperasjoner og byggteknikk på NTNU i Ålesund.

Vi ønsker først og fremst å uttrykke en stor takknemlighet til vår veileder Marie Haugli Larsen, som har loset oss gjennom forskningsprosjektet og utformingen av bacheloroppgaven. Gjennom alle deler av forskningsprosjektet har hun vært tilgjengelig og vist høy interesse for å gi gode og konstruktive tilbakemeldinger, noe som har vært av signifikant for gjennomføring av bacheloroppgaven. Videre ønsker vi å takke alle intervjupersoner for å ha satt av tid til intervju og bidratt med informasjon til forskningsprosjektet.

Vi begynte på denne bacheloroppgaven med begrensede forkunnskaper angående temaet: «digitalisering knyttet til sikker drift og cybersikkerhet på fartøy» og om akademisk oppgaveskriving, og ser derfor tilbake på dette forskningsprosjektet som meget lærerikt og opplysende. Valget av tema for forskningsprosjektet kom naturlig for oss, da dette for tiden er et svært aktuelt og sentralt tema for den maritime næringen så vel som mange andre næringer i denne samtidens stadig mer digitaliserte hverdag.

Vi håper at dette forskningsprosjektet vil belyse forholdet den maritime næringen har til digitalisering og hvordan dette oppleves å påvirke sikker drift og cybersikkerhet på fartøy. Videre, ved å undersøke hvorvidt digitaliseringen sitt helhetlige bidrag oppleves å gi flest fordeler eller ulemper for den maritime næringen, har forskningsgruppen også ambisjoner om at studien skal styrke beslutningsgrunnlaget og følgelig være til nytte for maritime aktører i kommende prosesser knyttet til digitalisering i maritim næring.

Magnus Gjerde, Andreas Sørum og Andreas Mulelid Kvam

# SAMMENDRAG

**Bakgrunn:** I kjølvannet av denne samtidens fokus på digitalisering og cybersikkerhet i samfunnet for øvrig, har proaktive maritime aktører gjennom de siste årene utvidet egne horisonter angående hvordan hensiktsmessig digitalisering kan fremme sikker drift parallelt med at cybersikkerheten på fartøy bevares.

**Formål:** Formålet med dette forskningsprosjektet er å undersøke forholdet den maritime næringen har til digitalisering og hvordan dette oppleves å påvirke sikker drift og cybersikkerhet på fartøy. Studien ønsker også å belyse hvorvidt digitaliseringen sitt helhetlige bidrag oppleves å gi flest fordeler eller ulemper for den maritime næringen.

**Problemstilling:** Hvordan opplever den maritime næringen at digitalisering påvirker sikker drift og cybersikkerhet på fartøy?

**Teori:** Det vil først presenteres teori angående digitalisering. Videre blir teori omhandlende sikker fartøydrift presentert. Deretter blir teori omhandlende cybersikkerhet beskrevet. Etter dette blir teori angående menneskelige faktorer beskrevet. Til slutt blir teori om opplæring på fartøy presentert.

**Metode:** Det har blitt benyttet kvalitativ metode med dybdeintervju. Studiens utvalg består av to dekksoffiserer og to rederiansatte fra forskjellige rederier i tillegg til én ansatt i et maritimt teknologiselskap. Forskningsprosjektets datamateriale har blitt fremstilt gjennom transkripsjon av lydopptak fra intervju og deretter analysert etter metoden systematisk tekstkondensering.

**Resultat:** Funnene i denne studien viser at den maritime næringen opplever at digitalisering medfører flere fordeler enn ulemper, og at digitalisering har bidratt med å fremme sikker fartøydrift. Funnene viser samtidig at det foreligger en bevissthet angående utfordringer digitalisering kan medføre for cybersikkerheten på fartøy, men at det er et varierende kompetansegrunnlag knyttet til bevaring av cybersikkerhet.

**Konklusjon:** Digitalisering fremmer sikker fartøydrift, men kan skape utfordringer knyttet til cybersikkerheten på fartøy om mannskapet ikke har et tilstrekkelig kompetansegrunnlag for bevaring av cybersikkerhet, og digitaliseringen må derfor balanseres med tilfredsstillende opplæring i cybersikkerhet.

**Nøkkelord:** digitalisering, sikker fartøydrift, cybersikkerhet, menneskelige faktorer, opplæring på fartøy, drivkrefter, utfordringer og kompetansegrunnlag

# SUMMARY

**Background:** In the wake of the present focus on digitalisation and cyber security in general society, proactive maritime players have in recent years expanded their own horizons regarding how appropriate digitalisation can promote safe operation in parallel with preserving cyber security on vessels.

**Purpose:** The purpose of this research project is to investigate the maritime industry's relationship towards digitalisation and how this is perceived to affect safe operation and cyber security on vessels. The study will also shed light on whether digitalisation's overall contribution is perceived to provide the most advantages or disadvantages for the maritime industry.

**Research question:** How does the maritime industry find that digitalisation affects safe operation and cyber security on vessels?

**Theory:** Theory regarding digitalisation will be presented first. Furthermore, theory regarding safe vessel operation will be presented. Then, theory regarding cyber security will be described. After this, theory regarding human factors will be described. Finally, theory about training on vessels will be presented.

**Method:** Qualitative method with in-depth interviews has been used. The study's selection consists of two deck officers and two shipping company employees from different shipping companies in addition to one employee in a maritime technology company. The research project's data material has been produced through transcription of audio recordings from interviews and then analyzed according to the method of systematic text condensation.

**Findings:** The findings of this study show that the maritime industry finds that digitalisation brings more advantages than disadvantages, and that digitalisation has contributed to promoting safe vessel operation. At the same time, the findings show that there is an awareness of challenges digitalisation can entail for the cyber security of vessels, but that there is a varying competence base associated with the preservation of cyber security.

**Conclusion:** Digitalisation promotes safe vessel operation, but can create challenges related to the cyber security of vessels if the crew does not have an adequate competence base for the preservation of cyber security, and digitalisation must therefore be balanced with satisfactory training in cyber security.

**Key words:** digitalisation, safe vessel operation, cyber security, human factors, training on vessels, driving forces, challenges and competence base

# TERMINOLOGI

| | |
|---|---|
| BIMCO | The Baltic and International Maritime Council (Store norske leksikon, 2020) |
| Cybersikkerhet | Cybersikkerhet er en utvidelse av fagområdet datasikkerhet, som også tar for seg IT-baserte enheter og infrastruktur. Cybersikkerhet fokuserer på internett-relaterte trusler (Heine Nätt, 2022). |
| Digitalisering | Digitalisering er det å legge til rette for generering av digital informasjon samt håndtering og utnyttelse av informasjonen ved hjelp av informasjonsteknologi (Dvergsdal, 2021). |
| Document of Compliance (DOC) | Et godkjenningsbevis utstedt til et selskap som overholder kravene i ISM-koden (Wikipedia, 2022). |
| Dynamisk Posisjonering (DP) | Dynamisk Posisjonering er at rigger, fartøyer, eller lignende holdes i posisjon på arbeidsstedet ved hjelp av flere propeller i stedet for ankere (Store norske leksikon, 2020). |
| Hacking | Hacking er et begrep som ofte benyttes synonymt med datakriminalitet og tekniske angrep mot maskiner og tjenester (Heine Nätt, 2022). |
| Patching | Patching er en prosess for å reparere en sårbarhet eller feil som identifiseres etter utgivelsen av en applikasjon eller programvare (Itarian, 2022). |
| Proxy | Proxy blir brukt som forkortelse for proxyserver, som er et mellomledd mellom en klient og en server, og som filtrerer, behandler og lagrer informasjon, vanligvis for bedre ytelse, hemmelighold eller sikkerhet (Nilstun, 2021). |

# INNHOLD

# FIGURLISTE



# TABELLISTE

# 1.0 INNLEDNING

Den internasjonale skipsfartsorganisasjonen BIMCO uttrykker at sjøfarten er i økende grad avhengig av digitale løsninger for å fullføre dagligdagse oppgaver (BIMCO, 2020). Digitalisering har derfor i de siste årene vært et sentralt tema for maritime aktører. BIMCO (2020) uttrykker videre at den raske utviklingen innen informasjonsteknologi, datatilgjengelighet, prosesseringshastighet og dataoverføring gir aktører i den maritime næringen økte muligheter for sikkerhetsforbedringer, driftsoptimalisering, kostnadsbesparelser og et mer bærekraftig virke (BIMCO, 2020).

I en melding til stortinget for perioden 2020 til 2021 fra Nærings- og fiskeridepartementet blir det beskrevet at norsk maritim næring har vært gjennom en utfordrende periode siden 2014, særlig knyttet til et krevende offshoremarked og lavere oljepris (Nærings- og fiskeridepartementet, 2020). Videre blir det uttrykt at til tross for et utfordrende marked er norsk maritim næring fortsatt ledende innenfor spesialiserte segmenter internasjonalt, der avansert teknologi og høy kompetanse kan veie opp for et høyt kostnadsnivå (Nærings- og fiskeridepartementet, 2020). Det er et tydelig engasjement for digitalisering i den norske maritime næringen, og i en Fafo-rapport utført på oppdrag av Norges Rederiforbund og Norsk Sjøoffisersforbund beskrives det at historisk, har det vist at utfordrende perioder for norsk maritim næring også har potensial for innovasjon og følgelig vekst (Andersen, Bjørnset, & Rogstad, 2019).

Utviklingen innenfor digitalisering er derimot i stor grad avhengig av økt tilkobling, ofte via internett mellom servere, IT og OT systemer, noe som også øker de potensielle sårbarhetene og risikoene for cybersikkerheten (BIMCO, 2020). Det er derfor viktig at den norske maritime næringen har et forhold til cybersikkerhet, der det tilrettelegges for et tilstrekkelig kompetansegrunnlag for bevaring av cybersikkerheten. IMO-resolusjon MSC.428(98), med navnet *Maritime Cyber Risk Management in Safety Management Systems* oppfordret for øvrig administrasjoner til å sikre at cyberrisiko ble hensiktsmessig adressert i sikkerhetsstyringssystemet senest ved første årlige verifisering av selskapers Document of Compliance etter 1. januar 2021 (IMO, 2017).

## 1.1 PROBLEMSTILLING

I belysning av valgt tema: «digitalisering knyttet til sikker drift og cybersikkerhet på fartøy», har vi utarbeidet følgende problemstilling:

*«Hvordan opplever den maritime næringen at digitalisering påvirker sikker drift og cybersikkerhet på fartøy?»*

Ved å intervjue to dekksoffiserer på fartøy, to kontoransatte på rederikontor og én ansatt i et maritimt teknologiselskap, har vi som formål for dette forskningsprosjektet å undersøke forholdet den maritime næringen har til digitalisering og hvordan dette oppleves å påvirke sikker drift og cybersikkerhet på fartøy. Studien ønsker også å belyse hvorvidt digitaliseringen sitt helhetlige bidrag oppleves å gi flest fordeler eller ulemper for den maritime næringen.

## 1.2 AVGRENSNINGER

Dalland (2012) forklarer at man enklere finner relevant litteratur for forskningsprosjektet ved å avgrense oppgaven. Forskningsgruppen anser forskningsprosjektet sin problemstilling til å være aktuell for den maritime næringen på et globalt plan, og at en forskningsprosess der man hadde involvert intervjupersoner fra flere stater enn Norge hadde vært mest hensiktsmessig for å oppnå et absolutt best forskningsresultat. Med forskningsprosjektets tidsbegrensninger blir dette likevel vurdert som lite hensiktsmessig, og forskningsgruppen har derfor satt avgrensninger for forskningsprosjektet.

Dette forskningsprosjektet er derfor i første omgang avgrenset til å omhandle norske dekksoffiserer på norskregistrerte fartøy, norske kontoransatte fra norske rederikontor og en norsk representant fra et norsk maritimt teknologiselskap. Videre er forskningsprosjektet avgrenset til å omhandle de representantene fra de ulike representantgruppene som har relevant og fersk arbeidserfaring knyttet til digitalisering i maritim næring. Forskningsgruppens nettverk av kontakter og forskningsprosjektets tidsbegrensninger har vært sentralt i beslutningen om å avgrense forskningsprosjektet til å gjelde intervjupersoner basert i Norge. Forskningsgruppen anerkjenner at denne avgrensningen kan ha hatt innvirkning på forskningsprosjektets funn, men vurderer det slik at man uavhengig de satte avgrensningene, endog kan fremstille interessante og relevante resultater.

## 1.3 OPPGAVENS OPPBYGNING

Bacheloroppgaven består av seks hovedkapitler. I bacheloroppgavens innledning blir oppgavens problemstilling og avgrensninger omkring den beskrevet. Deretter blir teori vurdert som relevant for bacheloroppgaven presentert i kapittelet for det teoretiske grunnlaget. Etter dette, blir det i kapittelet angående metode beskrevet hvilken forskningsmetode som har blitt benyttet for innsamling og analysering av oppgavens datamateriale. Deretter blir de fremstilte resultatene for forskningsprosjektet etter analyseprosessen beskrevet i kapittelet for resultat. I

det påfølgende kapittelet omhandlende drøfting, blir resultatene drøftet opp mot oppgavens problemstilling og det teoretiske grunnlaget. I det siste kapittelet blir bacheloroppgaven avsluttet med betraktninger angående de opplevde påvirkningene digitalisering har hatt for sikker drift og cybersikkerhet på fartøy, i tillegg til en vurdering av hvorvidt digitaliseringen sitt helhetlige bidrag oppleves å gi flest fordeler eller ulemper for den maritime næringen.

# 2.0 TEORETISK GRUNNLAG

I dette kapittelet vil det teoretiske grunnlaget i form av relevant litteratur om forskningsprosjektets overordnede hovedtema: «digitalisering knyttet til sikker drift og cybersikkerhet på fartøy» bli gjennomgått. Det teoretiske grunnlaget blir senere i oppgaven benyttet for å drøfte resultatene for forskningsprosjektet. Først presenteres teori angående digitalisering. Deretter vil kapittelet ta for seg teori om sikker fartøydrift. Etter dette vil teori om cybersikkerhet bli beskrevet. Videre vil det bli presentert teori omhandlende menneskelige faktorer. Deretter blir kapittelet avsluttet med teori angående opplæring på fartøy.

## 2.1 DIGITALISERING

Digital21 beskriver at digitalisering omhandler å ta i bruk mulighetene som digitale løsninger gir til å forbedre, fornye og skape nytt (Digital21, 2018). Dvergsdal (2021) uttrykker at: «Digitalisering er det å legge til rette for generering av digital informasjon samt håndtering og utnyttelse av informasjonen ved hjelp av informasjonsteknologi».

Det blir i rapporten fra Digital21 med navnet *Digitale grep for norsk verdiskaping* uttrykt at det er flere forhold som driver digitaliseringen fremover, der det blir for omfattende å presentere en fullstendig analyse av drivkreftene bak digitaliseringen. Videre beskrives det derfor at en stor drivkraft de siste femten årene har vært produksjon av, tilgang på og utnyttelse av data (Digital21, 2018).

Digital21 uttrykker at det er ingen tvil om at utviklingen angående digitalisering vil fortsette i mange år fremover (Digital21, 2018). Digitalisering er derfor et anliggende som de fleste organisasjoner i denne samtiden har et forhold til og prøver å benytte på en hensiktsmessig måte for å enklere oppnå organisasjoners formål, og digitalisering har derfor i de siste årene vært et sentralt tema i maritim næring. Rederier har i en lengre periode vist interesse for å bedrive digitalisering for å oppnå målsetninger som både sjø- og landsiden i et rederi har for sikker fartøydrift.

En type digitalisering er bruken av datamaskiner for å samle inn større datamengder og lagre dem over lengre tid, der dataene kan analyseres og brukes til å fremstille prediksjoner angående hvordan noe vil utvikle seg fremover i tid basert på tidligere data. Utviklingen innenfor digitalisering der horisonten bestandig utvides når det gjelder hvordan man kan bruke et datamateriale, gjør det samtidig noen ganger vanskelig å betrakte den fremtidige verdien av datamaterialets informasjon (Dvergsdal, 2021). Dvergsdal (2021) forklarer videre at det ikke

finnes noen oppskrift for å lykkes med digitalisering, og at det også er vanskelig å anskaffe en oversikt over eventuelle påvirkninger av digitalisering. Dvergsdal (2021) forteller videre at grunnen til at det er vanskelig å få overblikk over eventuelle effekter som følge av digitalisering, blant annet angår det at teknologien bestandig blir benyttet i nye sammenhenger og fordi påvirkningene ofte oppstår i samspill med andre faktorer. Dvergsdal (2021) uttrykker at det dog er noen sentrale effekter av digitalisering som går igjen i mange sammenhenger, og nevner at dette er økt uttrykkskraft, løsere tid- og stedbindinger og stabilitet og forutsigbarhet.

Økt uttrykkskraft omhandler at tallstørrelser i en datamaskin er løsrevet fra virkeligheten. Dette medfører at de ikke er bundet til et bestemt fysisk medium, noe som gjør at de kan brukes til å skape mange forskjellige fysiske uttrykk (Dvergsdal, 2021). Ved økt uttrykkskraft forteller Dvergsdal (2021) at man kan benytte omfattende og komplekse datamengder innsamlet av forskjellige måleinstrumenter til å fremstille avanserte statistikker på en hensiktsmessig måte slik at innholdet i statistikkene kan begripes av de fleste og anvendes til ønskede formål.

Løsere tid- og stedbindinger omhandler at tallstørrelser henimot er uavhengige av tid og sted. Dette vil si at informasjonen som tallmaterialet representerer fremdeles vil ha tid- og stedbindinger, men at informasjonen nå kan behandles på kortere tid og med mindre ressursbruk enn tidligere. Ved løsere tid- og stedbindinger kan man bruke datamaskiner til å innsamle store tallmengder og lagre dem i lang tid (Dvergsdal, 2021). Dvergsdal (2021) forklarer at dette kan ha stor nytteverdi fordi at dette blant annet muliggjør at man kan finne tilbake til gammel informasjon.

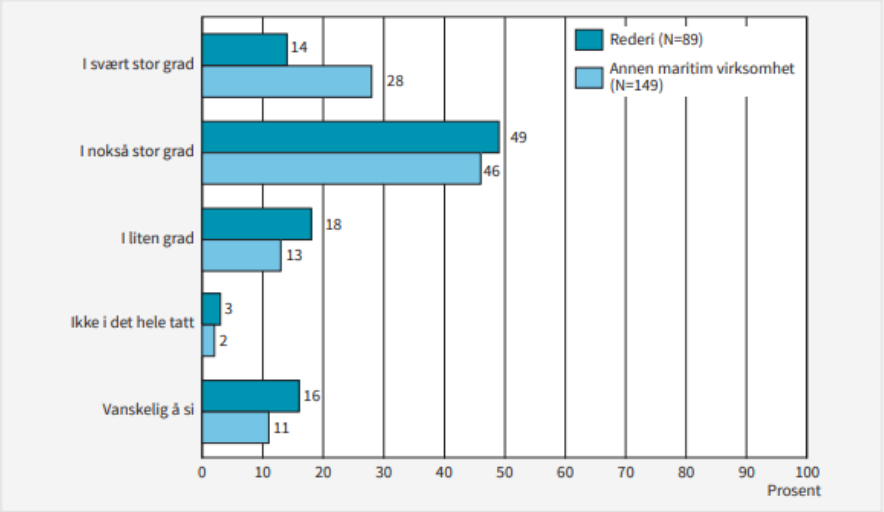
Stabilitet og forutsigbarhet omhandler at datamaskiner styres av algoritmer og at tallmaterialet de opererer derfor alltid er en forenklet utgave av virkeligheten. På bakgrunn av dette vil derfor alt foregå innenfor et matematisk definert rammeverk, både når det gjelder hva som skjer og hvilken sammenheng det skjer i (Dvergsdal, 2021). Dvergsdal (2021) uttrykker at dette rammeverket kan være enten tydelig og påtrengende der det er avgrenset hvilken informasjon som passer rammeverket, eller så kan rammeverket være mindre synlig der avgrensningene er usynlige for folk flest.

### 2.1.1 DIGITALISERING I MARITIM NÆRING

Norges Rederiforbund beskriver digitalisering i maritim næring til å omhandle å ta i bruk teknologi for å sikre effektive operasjoner, redusere kostnader, øke sikkerheten eller skape nye tjenester og markeder (Norges Rederiforbund, n.d.). Norges Rederiforbund uttrykker videre om Norge som nasjon tar lederrollen i å utvikle ny digital teknologi kan man samtidig skape

verdier og arbeidsplasser, der de som kommer raskt i gang med digitalisering vil ha et tydelig konkurransefortrinn internasjonalt (Norges Rederiforbund, n.d.).

I en rapport utarbeidet av Fafo på oppdrag av Norges Rederiforbund og Norsk Sjøoffisersforbund med navnet *Maritim kompetanse i en digital framtid* blir det i en spørreundersøkelse undersøkt hvordan den norske maritime næringen mente utviklingen innenfor digitalisering ville bidra med å styrke verdiskapingen i deres virksomhet. Denne undersøkelsen viser at det er en stor tro på at digitalisering vil kunne styrke verdiskapingen for virksomhetene i maritim næring, der 63 prosent av rederiene og 73 prosent av de andre maritime virksomhetene mener at dette kan bidra i svært stor eller nokså stor grad. På samme tid viser undersøkelsen en usikkerhet i den maritime næringen angående hvorvidt digitalisering vil styrke verdiskapingen i egen virksomhet. Undersøkelsen viser også at det er en andel som ikke har tro på at digitalisering vil medføre verdiskaping i deres virksomhet, men denne andelen utgjør endog et betydelig mindretall (Andersen, Bjørnset, & Rogstad, 2019).




*Figur 1: I hvilken grad kan digitalisering bidra til å styrke verdiskapingen i din virksomhet? (Andersen, Bjørnset, & Rogstad, 2019)*

I en annen rapport utarbeidet av Digital21 med navnet *Digitale grep for norsk verdiskaping* blir det uttrykt at når det gjelder å utnytte mulighetene som digitalisering medfører, så er den maritime næringen er en av de ledende bransjene i Norge. Digital21 forklarer videre at den norske maritime næringen også er i toppsjiktet internasjonalt på mange områder og forklarer at denne posisjonen internasjonalt kan tilskrives kombinasjonen av kompetente sjøfolk, risikovillige rederier og teknologiledende verft og skipsutstyrsbedrifter og verdensledende forsknings- og utdanningsmiljøer med sterk innovasjonsevne (Digital21, 2018).

Det beskrives i Fafo-rapporten at angående digitalisering i maritim næring så er det ikke autonome og førerløse fartøy som er det mest presserende for informantene som har bidratt til rapporten. Videre forklarer informantene at når det gjelder digitalisering i maritim næring, så er de i stedet opptatt av hvordan de kan kombinere ny teknologi og økende automatisering for å kunne behandle store mengder informasjon for å kunne oppnå en rekke optimaliseringsgevinster. Informantene forklarer videre at disse fordelene er knyttet til drift, innovasjon og nye forretningsmodeller (Andersen, Bjørnset, & Rogstad, 2019).

Rapporten fra Fafo forklarer videre at digitalisering representerer et betydelig potensial for den maritime næringen. Samtidig blir det nevnt at en større del av den maritime næringen mangler digital kompetanse. Det kommer også frem at rundt syv av ti fra både rederi og annen maritim næring gir uttrykk for at det i stor eller noen grad er en manglende digital kompetanse i egen virksomhet. Det uttrykkes også at det er en usikkerhet i den maritime næringen når det gjelder hvilken teknologi som eventuelt skal investeres i angående digitalisering. Videre blir dette beskrevet at denne typen usikkerhet fordrer en strategisk ledelse i hver enkelt virksomhet. Rapporten beskriver videre at det i den sammenhengen er relevant å bemerke at ulike maritime aktører vil ha ulike nytter fra de tilgjengelige digitale løsningene. Det blir også poengtert i rapporten at digitalisering for noen maritime aktører oppleves å medføre store kostnader der det forklares videre at dette særlig gjelder om det investeres i feil teknologi, samtidig som det av andre maritime aktører blir uttrykt at de har råd til å gjøre feilinvesteringer (Andersen, Bjørnset, & Rogstad, 2019).

I rapporten fra Fafo blir det også tatt opp hvordan digitalisering kan påvirke bemanningen på fartøy, der det uttrykkes at krav til bemanning på fartøy er knyttet til sikkerhet, og at sikkerhet derfor er sentralt diskusjoner om digitalisering. Rapporten uttrykker videre at det i utgangspunktet er Sjøfartsdirektoratet som bestemmer sikkerhetsbemanning på fartøy, i henhold til forskrift om bemanning av norske skip, og forklarer videre at sikkerhetsbemanning på fartøy angår den minste tillatte bemanning som et fartøy kan ha ved operasjon. Eventuelle endringer i bemanning på fartøy kan påberope at man først må tilrettelegge for en mer effektiv fartøydrift gjennom digitalisering om man fortsatt skal kunne bedrive sikker fartøydrift. Det blir i rapporten fra Fafo videre uttrykt at digitalisering vil medføre et økt fokus på system- og elektronikkompetanse, der kapteinen kanskje ikke vil ha samme rollen som før. Videre beskrives det at kapteiner derfor kanskje blir mer arbeidsledere og at det viktige sjømannskapet vil bli mer overlatt til systemene. Det beskrives videre at dette kan gjøre at kapteinen kan bruke

mer tid på andre saker som god ledelse og effektivisering av oppgavene som gjøres om bord på fartøyet og ved kai (Andersen, Bjørnset, & Rogstad, 2019).

Med økende datainnsamling på fartøy vil kunne fremstille store mengder data, der man gjennom riktig analyse av datamaterialet vil kunne øke effektiviteten av fartøydriften. Videre beskrives det at digitalisering kan brukes til å frembringe store endringer knyttet til vedlikehold, der digitalisering og bedre utstyr for monitorering av fartøykomponenters helsestatus vil tillate og gå fra preventivt til reaktivt vedlikehold på fartøykomponentene (Andersen, Bjørnset, & Rogstad, 2019).

Digitalisering kan sette sjøfolk i en helt ny arbeidssituasjon som følger av implementering av flere digitale funksjoner, der det videre blir beskrevet at digitalisering muliggjør at mye kan fikses ved fjerntilgang til fartøyet fra land. Det blir videre poengtert at det endog finnes problemer som ikke kan løses gjennom fjerntilgang til fartøy fra land, der det forklares at det derfor er nødvendig med folk som innehar fagekspertise fysisk om bord på fartøyet for å kunne utbedre eventuelle problemer med digitale løsninger. Dette støttes opp med at rapporten fra Fafo fant at 97 prosent er helt eller delvis enige i at fremtidens sjøfolk må inneha både digital kompetanse og den maritime. Videre er det også stor enighet om at sjøfolkene må ha kunnskaper om å oppdatere, vedlikeholde og reparere de digitale løsningene på fartøy (Andersen, Bjørnset, & Rogstad, 2019).

### 2.1.2 DRIVKREFTER FOR DIGITALISERING I MARITIM NÆRING

I en studie fra telekommunikasjonsselskapet Inmarsat, med navnet *Digitalisation Uncovered: What's Next for Shipping?* ble det gjennom en kvantitativ undersøkelse fremstilt en rekke ulike drivkrefter for implementering av digitale løsninger i den maritime næringen. I denne oversikten, kan man observere noen drivkrefter, der tre betydelige drivkrefter er: forbedring av tryggheten på fartøy, overholdelse av lovkrav og reduseringer av driftskostnader (Inmarsat, 2020, p. 15). BIMCO (2022) uttrykker i et innlegg om maritim digitalisering at det i samtidens maritime næring er et sterkt fokus på utvikling av nye teknologiske løsninger, der digitaliseringsmulighetene er særlig aktuelle. BIMCO (2022) antyder tre sentrale drivkrefter for digitalisering: konkurransepress for kostnadseffektivitet, miljøfaktorer med tilhørende lovkrav og interessenters økende krav til digitalisering. BIMCO (2022) forklarer videre at graden av digitalisering som anses hensiktsmessig varierer med hensyn til fartøystype, handelsmønster og operasjonsområde.

### 2.1.3 BRUKSOMRÅDER FOR DIGITALISERING I MARITIM NÆRING

Når det gjelder bruksområder for digitalisering i maritim næring, deler Inmarsat dette inn i noen kategorier: navigasjon, flåteprestasjon, risiko og sikkerhetsstyring, andre flåteoperasjoner, forsikring og mannskap (Inmarsat, 2020, pp. 21-23, 28-31). Dette viser det brede spekteret av bruksområder der digitalisering kan påvirke den maritime næringen. Samtidig som digitalisering har mange bruksområder for den maritime næringen, fant også Inmarsat studien at den maritime næringen var usikker angående hvorvidt digitalisering ville gi valuta for pengene eller bare øke den overhengende risikoen for cyberangrep (Inmarsat, 2020).

## 2.2 SIKKER FARTØYDRIFT

Sikker drift av fartøy står sentralt i rederiers ønskede målsetninger for ivaretakelse av liv, helse, miljø og andre verdier. Å drifte fartøy på en sikker måte krever bred kompetanse i fra begge parter i rederiet, både på sjøen og på land (Borch, 2016).

Driften av et fartøy preges av klare oppgaver og ansvar i fra ulike avdelinger om bord, inkludert fra de som sitter på land. I boken *Fartøysledelse og kontroll av skipets drift* av Odd Jarl Borch beskrives et fartøy som: «Et lite samfunn i miniatyr, der alle er avhengige av hverandre og arbeider og bor i et fellesskap». Som leder har du ansvar for at de som er om bord er trygge og har det bra til enhver tid. Samtidig skal en ta vare på de store verdiene som fartøy og last representerer, og utføre oppgavene effektivt uten skader. Dette krever god oversikt, handlingsevne og en god utnyttelse av det personell en har om bord i de ulike avdelinger og stillinger (Borch, 2016). Dette bringer oss videre på det med sikkerhetskultur og hvorfor det er så viktig med en god sikkerhetskultur både på fartøy og i selskapet som drifter det.

### 2.2.1 SIKKERHETSKULTUR

For å drifte et fartøy effektivt, men samtidig å beholde sikkerhetsaspektet ved dets oppgaver på sjø og i havn, er det viktig å ha god sikkerhetskultur både på fartøy og i rederiet. Sikkerhetskultur kan defineres som: «Etablerte verdier, holdninger og handlingsmønstre blant de ansatte, som bidrar til at en er vaktsom og kontinuerlig på søking etter tiltak for å redusere risiko for uønskede hendelser, med en følelse av kollektivt ansvar og en verdsetting av mål, virkemidler og styringssystemer for å redusere risiko» (Borch, 2016). Utviklingen av en slik sikkerhetskultur er krevende for ledelsen både i rederi og på fartøy i den forstand at dette må komme fra en indre personlig motivasjon. Og da er det viktig at det i ledelsen om bord på fartøy og i rederiet generelt går frem som gode eksempler da ledere som oftest har stor påvirkning på andre ansattes sikkerhetsatferd. Hvordan en leder prioriterer og engasjerer seg, samt deres

kompetansenivå angående sikkerhet har stor betydning for de ansattes sikkerhet. Sikkerhetsarbeidet må derfor starte på toppen av organisasjonen, og ifra et fartøy sitt ståsted vil dette være kaptein, overstyrmann og offiserer generelt (NHO, 2017).

### 2.2.2 SIKKERHETSLEDELSE

Borch beskriver at det er viktig at en ikke ser på sikkerhetsledelse som et ritual knyttet til slavisk det å følge regler, prosedyrer og styringsverktøy, men at det er nødvendig med en helhetlig tilnærming der godt sjømannskap og skjønn blir brakt inn og bygger opp grunnleggende verdier og holdninger som gjør at sikkerheten blir en naturlig del av arbeidet (Borch, 2016). God sikkerhetskultur handler også om hvorvidt rederiet eller fartøyet kan utvikle seg og lære av dets feil, ulykker og hendelser. Å ha god sikkerhetskultur kan da igjen beskrives som et kontinuerlig arbeid som aldri tar slutt (Borch, 2016).

Men hva er god sikkerhetskultur uten sikkerhetsledelse. Borch beskriver at sikkerhetsledelse kan defineres som beslutning, iverksetting, styring og kontroll rettet mot å redusere risiko knyttet til liv, helse, miljø og andre verdier. Dette vil i bunn og grunn innebære isolasjon av risikofaktorene som ikke kan fjernes og å sette mål og akseptkriterier for risikoen om bord i fartøyet. Som nevnt er sikkerhetsarbeidet på fartøy en kontinuerlig aktivitet der en både skal være proaktiv rettet mot å oppdage, fjerne eller redusere risiko før noe uønsket skjer, være aktiv ved å eliminere effekten av uønskede hendelser og reaktiv ved å ta hensyn til erfaringer fra tidligere ulykker og hendelser. Fra et fartøys ståsted innebærer dette at en må starte arbeidet med sikkerhetsledelse allerede under planlegging og bygging av fartøyet og gjøre dette til en løpende prosess ved overtakelse av fartøyet og føre dette inn i driften (Borch, 2016, s. 206 og 207). Sikkerhetsledelse baserer seg på en rekke faktorer ifølge Borch (2016):

1. Den første faktoren dreier seg om at man må bygge seg opp en filosofi om at risikoarbeidet om bord er noe som kan være mulig å styre og at det skal være mulig å bygge opp vaner og handlingsmønstre der en tar ansvar for og har fokus på trygghet i alt en gjør.
2. Den andre faktoren dreier seg om å få til mentale prosesser som gjør at en får opp bevisstheten om risiko og hva som kan gå galt samt aktiv handling som respons på risiko og uønskede hendelser.
3. Den tredje faktoren omhandler at sikkerhetsledelsesarbeidet om bord er tett tilknyttet arbeidsmåter der en utvikler rutiner og vaner med fokus på å skape stadig tryggere omgivelser og være forberedt på å takle uønskede hendelser.
4. Den fjerde faktoren angår et helhetlig blikk på ledelse, som går ut over fartøyets grenser.

I sikkerhetsarbeidet henger alt sammen med alt, og vi er sterkt avhengig av at dem som vi samhandler med både på land og sjø også gjør en innsats for å få til sikker drift (Borch, 2016, s. 206 og 207).

### 2.2.3 CYBERSIKKERHETSKULTUR

Det er viktig at sikkerhetskulturen om bord i fartøy i dag også inkluderer cybersikkerhet. Selskapet PricewaterhouseCoopers (PwC) skriver på sine nettsider at: «Sikkerhetskulturen er et virkningsfullt og naturlig virkemiddel for bevisstgjøring rundt informasjonssikkerhet. Sikkerhetskulturen vil ikke minst bidra til å understreke hvor viktig det er at alle tar del i forsvaret mot cyberangrep. Ved å kombinere teknologi, gode interne prosesser og menneskelig opplæring via sikkerhetskultur gjør man jobben til trusselaktørene betydelig vanskeligere» (PwC). Målet bør være at sikkerheten skal bli forankret høyt først og fremst hos ledelsen, slik at de kan gå frem som gode eksempler, men også hos andre ansatte i selskapet. Sikkerhetskulturen vil innebære å jobbe med de ansatte, at risikoer rundt cybersikkerhet blir forstått og tatt på alvor samt at opplæringsmateriell- og programmer blir utarbeidet og spesifisert for alle roller og funksjoner i virksomheten (PwC, 2022).

## 2.3 CYBERSIKKERHET

«Cybersikkerhet er en utvidelse av fagområdet datasikkerhet, som også tar for seg IT-baserte enheter og infrastruktur. Cybersikkerhet fokuserer på internett-relaterte trusler. Cybersikkerhet er ikke direkte knyttet til informasjonen som oppbevares, men til tjenestene, systemene og infrastrukturen rundt. Ved å sikre disse vil i midlertidig også informasjonen indirekte sikres» (Heine Nätt, 2022).

Cybersikkerhet er viktig på grunn av den mulige effekten det kan ha på personell, fartøy, miljøet, selskapet og last. Cybersikkerhet omhandler beskyttelse av IT og OT system, informasjon og data fra uautorisert tilgang, manipulering og forstyrrelser (BIMCO, 2020, s. 3). ISM koden, støttet av IMO vedtak MSC.428(98), satte krav om at alle skipseiere og ledere skulle vurdere cyberrisikoen og iverksette relevante tiltak i alle funksjoner i deres sikkerhetssystem innen 1 januar 2021 (DNV).

### 2.3.1 SÅRBARHETER OG CYBERANGREP

Den maritime næringen har et stort spekter av karakteristikker som påvirker hvor sårbart det er for cyberangrep. Noen av disse karakteristikkene som beskrives er (BIMCO, 2020, s. 3):

- Involveringer av mange ulike aksjeeiere i det operasjonelle og befraktning av et skip kan føre til ansvarsfraskrivelse.

- Skipsutstyr som er fjernstyrt og åpnet, for eksempel av produsent eller støtteleverandører.
- Tilgjengeligheten og bruken av computerstyrte kritiske system, som kanskje ikke har den siste installeringen for å kunne tette sikkerhetshull, eller forsvarlig sikret, for skipets sikkerhet og miljøvern.
- En kultur for cyberrisikostyring som fortsatt har potensiale for forbedringer, gjennom mer formell trening, øvelser, og klare roller og ansvar.

Cyberangrep er noe alle selskaper i dagens samfunn kan bli utsatt for. Noen selskaper kan bli angrepet grunnet svakheter som blir oppdaget av angripere, mens andre bedrifter kan være spesifikke mål. Kjennskap til hvilken type angriper man har å gjøre med, kan gi deg innblikk i hvilke motivasjon og motiv som ligger bak angrepet (BIMCO, 2020). Vi skiller i all hovedsak mellom 5 typer cyberangripere (BIMCO, 2020, s. 13):

1. *Cyberkriminelle* er motivert av de samme tingene som andre kriminelle: penger eller andre gods. Cyberkriminalitet inkluderer identitetstyveri og utpressingsvare. Cyberkriminelle gjenger kan handle for egen fortjeneste eller leie ut sine tjenester.
2. *Cyberaktivister* er generelt motivert av filosofi, politikk eller ikke-økonomiske mål. Denne form for hackergrupper deltar i aktiviteter som feilinformasjon i sosiale medier eller endring av visuelt utseende på nettsteder.
3. *Cyberspioner* handler på vegne av rivaliserende selskaper eller nasjonsstater, cyberspioner deltar i finansielle, industrielle, politiske og diplomatisk spionasje, inkludert intellektuelt eiendomstyveri.
4. *Cyberterrorister* gjennomfører cyberangrep for politisk, religiøs, ideologisk, eller sosiale grunner, med motiv om å spre frykt hos målgruppen deres. Cyberterrorister kan være selvstendig eller jobbe som proxyer for nasjonsstater.
5. *Cyberkrigere* handler generelt på vegne av en nasjonsstat for å komme nærmere deres strategiske mål. Cyberkrigere jakter generelt militære eller kritiske infrastrukturer.

### 2.3.2 SYSTEMSIKRING

Mens IT-systemer administrer data og støtter forretningsfunksjoner, er OT maskinvaren og programvaren som direkte overvåker/kontrollerer fysiske enheter og prosesser og som sådan er en integrert del av fartøyet og må fungere uavhengig av IT-systemene om bord. Systemene kan imidlertid kobles til IT-nettverket for ytelsesovervåking, fjernstøtte og lignende. Slike systemer omtales noen ganger som tilhørende «Industrial Internet of Things» (IIoT). I slike tilfeller er det viktig å sikre at grensesnittet er tilstrekkelig bevoktet av en brannmur som et

minimum og mulige sårbarheter i OT-systemene ikke eksponeres i IT-nettverket. Dette er viktig fordi det ikke alltid er mulig eller gjennomførbart å sikre et riktig oppdateringsnivå i OT-systemer (BIMCO, 2020).

IT dekker spekteret av teknologier for informasjonsbehandling, inkluder programvare, maskinvare og kommunikasjonsteknologi. Tradisjonelt sett har OT og IT blitt separert, men internett har sørget for at OT og IT kommer nærmere hverandre, ettersom historisk frittstående systemer blir integrert. Forstyrrelser i driften av OT systemer kan føre til en betydelig risiko for sikkerheten til personell om bord, last, skade på det marine miljøet og hindre fartøyets drift. På samme måte kan svikt i visse IT- systemer, for eksempel mangel på umiddelbar tilgang til farlig gode, også skape farlige situasjoner. For eksempel, i situasjoner der en container ombord på et fartøy brenner, er informasjon om innholdet i containeren viktig for å avgjøre riktig brannslokking (BIMCO, 2020).

Det kan være forskjell på hvem som håndterer innkjøp av OT og IT systemer på et fartøy. IT ledere er vanligvis ikke involvert i kjøp av OT systemer, og har kanskje ikke en grundig forståelse av cybersikkerhet. Kjøp av slike systemer bør involvere noen som har forståelse for innvirkningen på systemene ombord, men de fleste har vanligvis begrenset kunnskap om programvare og cyberrisikostyring. Derfor er det viktig med dialog med en person som har kunnskap om cybersikkerhet for å vurdere cyberrisiko under OT kjøpsprosessen. Oppdatering av OT-programvare krever grundig kompatibilitetssjekk og klassegodkjenning, i motsetning til IT programvare. Derfor kan det være en fordel for den ansvarlige for cybersikkerhet ombord, å ha en beholdning av OT-systemer. Da er det lett å få oversikt over potensielle utfordringer, samt bidra med etablering av nødvendig politikk og prosedyrer for vedlikehold av programvaren (BIMCO, 2020).

Det er umulig for et rederi eller selskap å sikre seg helt mot cyberangrep, men det finnes mange gode tiltak for å redusere risikoen for et mulig angrep. «Det er nødvendig å tenke helhetlig for å beskytte mot dataangrep. Bruk av sterke passord og sikre autentiseringsmetoder er en del av grunnsikringen vi alle må gjøre for å beskytte oss» (NSM). Blant tiltakene som nevnt av BIMCO (2020) og National Cyber Security Center (u.d.) er oppdatering av programvare, segregering og gode passordrutiner.

Det er viktig å holde programmene ombord oppdaterte med siste tilgjengelige versjon av programmet. Dette er viktig for å unngå angrep som utnytter programvarefeil. Patching, som innebærer å tette sikkerhetshull, er en viktig del av sikring av systemer ombord, og gjøres i

form av oppdatering og vedlikehold av programvarene. Enheter som kobles til det sentrale nettverket ombord er å anse som endepunkt, og dermed ekstra utsatt for trusler da de ofte er det svakeste leddet i nettverkets sikkerhet. Det er derfor viktig med en eller flere typer beskyttelse i form av anti-virus programmer, brannmurer, data input/output kontroll, og program- brukeradministrasjon (BIMCO, 2020).

Segregering er en av de mest effektive metodene for å forebygge cyberhendelser og forhindre spredning av skadevarer er å hindre angripere tilgang til fartøysystemet. Dette oppnår man gjennom å segregere systemene eller nettverkene. Man kan for eksempel ha segregering mellom IT og OT systemene, ved at de er koblet opp til ulike servere eller nettverk. Det er også en fordel at man har flere V-LAN (virtuelle lokale områdenettverk) ombord, for å gruppere enheter etter hvilken tilgang de skal ha. Mannskapet bør for eksempel ha et eget nettverk ombord som er separat fra nettet som utstyret på broen er koblet til, slik at eventuelle skadevarer ikke skal spre seg fra private datamaskiner til serveren og strømstyringen ombord (BIMCO, 2020).

Gode passordrutiner er viktig. Boken *Datasikkerhet: ikke bli svindlerens neste offer* tar for seg viktigheten av gode passord. Ifølge (Heine Nätt & Heide, 2021) velger folk ofte passord som er lette å knekke, fordi hjernen ikke er konstruert for å lage tilfeldige tegnsammensetninger.

### 2.3.3 CYBERRISIKOSTYRING

«Risiko innebærer at hendelser kan inntreffe som har konsekvenser for noe som er av verdi for oss mennesker». «beskrivelse eller måling av risiko utføres i en risikoanalyse. Her spesifiseres hendelser som kan skje og deres konsekvenser. Risikoanalysen uttrykker også hvor trolige hendelsene er» (Aven, 2019). Vi kan derfor si at risikoen er ett mål på konsekvensen en hendelse kan ha, sett i forhold til sannsynligheten for at det skjer.

Cyberrisikostyring bør være en innboene del av et rederi sin trygghets- og sikkerhetskultur for å bidra til trygg og effektiv operasjon av fartøy. Videre bør cyberrisikostyring være iverksatt på ulike nivå i organisasjonen, inkludert personell om bord på fartøy og senior ledelsen på land. Cyberrisikostyring burde ifølge BIMCO (2020, s. 4):

- Identifisere roller og ansvar til brukere, nøkkelpersonell og ledelse både om bord og på land.
- Identifisere systemet, eiendeler, data og kapasitet som, hvis forstyrret, kan utgjøre risiko for fartøyets operasjon og sikkerhet.

- Implementere tekniske og prosedyremessige tiltak for å beskytte mot cyberangrep, rettidig oppdagelse av hendelser og sikre videre drift.
- Implementere en beredskapsplan som det trenes regelmessig på.

BIMCO (2020) har videre laget en modell for en tilnærming til cyberrisikostyring:


*Figur 2: Tilnærming til cyberrisikostyring som beskrevet i BIMCO sine retningslinjer for cybersikkerhet (BIMCO, 2020)*

## 2.4 MENNESKELIGE FAKTORER

I store selskaper som rederier og om bord i fartøyene som blir driftet av dem er det mange faktorer som skal opp til vurdering ut ifra et sikkerhetsståsted. Hvis ansvaret blir fordelt på mange personer er det lett for å overse faktorer som lett kan eskalere til å få katastrofale konsekvenser. Teknologien som blir tatt i bruk for å drifte fartøy er meget krevende og omgivelsene krever sitt både på sjøen og i havn. Det er derfor viktig å vite at selv om et rederi eller et annet selskap har høye ambisjoner og omfattende sikkerhetsstyringssystemer så kan

uhellet skje (Borch, 2016). Ifølge Borch (2016) dreier den menneskelige faktoren om evnen til å:

- Observere hva som skjer
- Fange opp signaler tidlig, bearbeide disse og gi mening til dem
- Forutsi utviklingen videre
- Koble en hendelse til et større hele om bord
- Bryte ut av vanetenkning og forstå og handle ut fra nye tankemønstre
- Være handlingsorientert og finne nye løsninger
- Trekke lærdom av hendelser

Videre beskriver Borch (2016) at hvordan mennesker observerer og handler påvirkes av en rekke faktorer:

- Utdanning
- Erfaring
- Våkenhet
- Organisering og egen posisjon
- Kommunikasjon mellom nivåene og avdelingene i organisasjonen
- Følelse av ansvar og myndigheten til individet
- Grunnleggende verdisett og normer for adferd
- Holdninger og meninger
- Respekt for andre
- Gruppepåvirkning

## 2.5 OPPLÆRING PÅ FARTØY

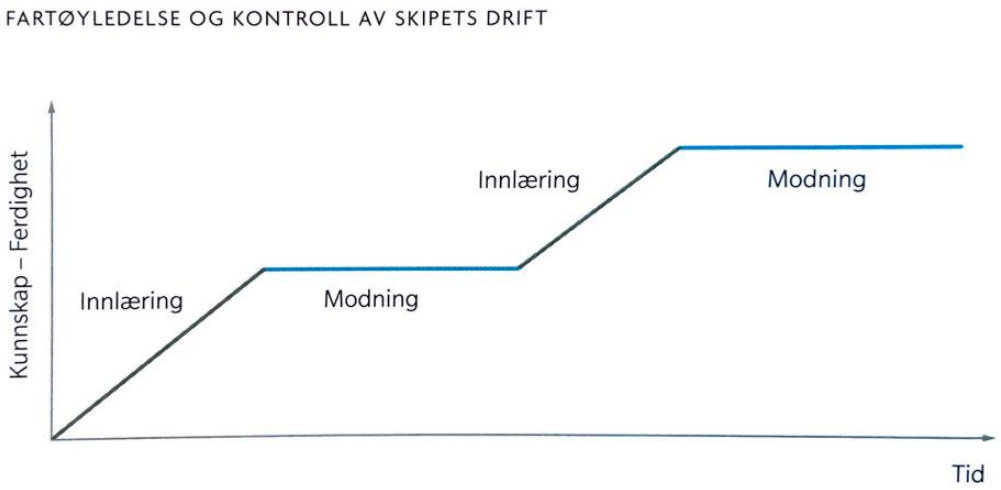
I henhold til regelverket påhviler det rederiet og skipsføreren et ansvar for at skipsbesetningen får og har tilstrekkelig opplæring i de oppgavene de settes til å utføre. Opplæring som dette skal gjentas regelmessig og også ved innføring av ny teknologi eller risikomomenter. For øvelser i forbindelse med fartøyets drift og sikkerhet er det egne regler for hvor ofte og i hvilken form disse skal avholdes (Borch, 2016).

For at opplæring skal fungere effektivt, er det viktig at den blir tilpasset det enkelte individet, noe som krever kartlegging av individets bakgrunn og tidligere erfaringer slik at en ikke bruker unødvendig tid på opplæring av individet angående kunnskap som individet allerede innehar.

Når en har kartlagt og skaffet seg klarhet i personens kunnskaper og erfaringer må en også prøve å forsøke å finne ut hvordan personen kan best ta til seg opplæringen han eller hun skal igjennom (Borch, 2016). I denne sammenheng beskriver Borch (2016) at det finnes tre ulike begreper for dette:

1. Den første er den *auditive*, som vil si læring ved å bli fortalt eller å lese om noe.
2. Den andre er den *visuelle* læringsstilen. Denne går ut på å lære ved å få noe illustrert og visualisert.
3. Den tredje er den *kognitive*, denne omtales ofte som «learning by doing» som vil si å lære ved å utføre noe.

På fartøy i dag er det som oftest en bukett med forskjellige personligheter og kulturer om bord. Alle individer tenker og prosesserer det man lærer ulikt. Ved innlæring av nye kunnskaper deler man gjerne denne prosessen inn i to deler, denne prosessen beskriver Borch som innlæring og modning. Sammenhengen i dette handler om at ny innlært kunnskap eller ferdigheter trenger tid til å modnes for å feste seg hos det enkelte individ. Hvor lang tid de forskjellige periodene med innlæring og modning vil ta, kommer helt an på kompleksiteten av det som skal læres og er selvsagt personavhengig (Borch, 2016). Borch (2016) har utarbeidet en lærekurve basert på dette:




*Figur 3: Lærekurven (Borch, 2016)*

Det er som nevnt tidligere viktig å kartlegge hvor et individ står i prosessen for å best tilegne individet et potensiale for god læring. Ny innlæring basert på mangelfullt grunnlag vil som regel ikke gi god læring og vil kunne føre til at ferdigheter og kunnskaper ikke vil sitte godt nok. Borch forteller videre at i operative sammenhenger, som de fleste sammenhenger om bord

på fartøy er, vil dette kunne føre til stygge uhell og ulykker. Ikke bare med tanke på liv, helse og miljø, men tatt i betraktning for cybersikkerheten også (Borch, 2016).

# 3.0 METODE

Den norske sosiologen Vilhelm Aubert, som sitert i (Dalland, Metode og oppgaveskriving, 2020, s. 53) beskriver metode som følgende: «En metode er en fremgangsmåte, et middel til å løse problemer og komme frem til ny kunnskap. Et hvilket som helst middel som tjener formålet, hører med i arsenalet av metoder» (Aubert, 1985).

Når det gjelder valg av metode beskriver Dalland videre at «Refleksjonene omkring valg av metode må komme klart frem» (Dalland, Metode og oppgaveskriving, 2020, s. 56). Dette kapittelet vil derfor først ta for seg valget av forskningsmetode og refleksjonene angående hvor godt denne metoden egner seg til forskningsprosjektets formål og problemstilling. Deretter vil forskningsgruppen gi en avklaring av egen forforståelse i forkant av forskningsprosjektet, etterfulgt av beskrivelser av forskningsprosjektets planlegging, utføring og analyse. Til slutt i dette kapittelet blir feilkilder for resultatene redegjort for.

## 3.1 FORSKNINGSMETODE

Argumentet som det må tas hensyn til når det gjelder valget av en bestemt forskningsmetode angår hvilken metode som forskningsgruppen selv mener vil kunne i størst grad egne seg til forskningsprosjektets formål og problemstilling (Dalland, Metode og oppgaveskriving, 2020, s. 53). Det ble derfor vektlagt tyngst hvilken forskningsmetode som forskningsgruppen selv vurderte ville være mest hensiktsmessig å benytte med hensyn til forskningsprosjektets formål for å bidra til belysning av problemstillingen på en best mulig måte.

Formålet til forskningsprosjektet er å undersøke forholdet aktører i den maritime næringen har til digitalisering og hvordan dette oppleves å påvirke fartøydriften og cybersikkerheten på fartøy. Dalland forklarer at de kvantitative metodene har som fordel at de får frem data i form av målbare enheter og at de kvalitative metodene tar sikte på å fange opp mening og opplevelse som ikke lar seg tallfeste eller måle (Dalland, 2020, s. 54). På bakgrunn av dette, har forskningsgruppen vurdert at kvalitativ metode vil være mest tilfredsstillende for forskningsprosjektet, da denne studien har som formål å fange opp meninger og opplevelser fra relevante intervjupersoner fra maritim næring som ikke lar seg kvantifisere.

## 3.2 AVKLARING AV EGEN FORFORSTÅELSE

«Vi har alltid våre fordommer eller vår forforståelse med oss inn i en undersøkelse» (Dalland, 2020, s. 60). En norm innenfor forskning beskriver at man skal være sin egen forforståelse bevisst angående alle faktorer som kan ha innflytelse på forskningen. Det er derfor essensielt

at man avklarer egen forforståelse i forkant av et forskningsprosjekt, slik at leseren er opplyst om forskningsgruppen sin posisjon innenfor forskningsområdet i vurderingen av forskningsvirksomheten sin validitet. Å avklare egen forforståelse vil også kunne hjelpe forskningsgruppen i å aktivt arbeide mot at egen forforståelse får påvirke forskningsvirksomheten i for høy grad i tolkning og bearbeiding av datamaterialet fra forskningsprosjektet, ved registrering av faktorer som kan ha innflytelse på forskningen. «Når vi har klargjort for oss selv hvilke tanker vi har om fenomenet på forhånd, er det lettere å lete etter data som eventuelt kan avkrefte disse» (Dalland, 2020, ss. 60-61).

Forskergruppen vår består av tre bachelorstudenter ved nautikkstudiet på NTNU i Ålesund. Den maritime bakgrunnen til forskningsgruppen er forskjellig. Én av tre har matrosfagbrev og sånn sett mest jobberfaring fra fartøy, mens de resterende to på gruppen bare i begrenset grad har jobbet på fartøy og derav har mindre jobberfaring fra fartøy. Ingen av oss har imidlertid noen utvidet arbeidserfaring angående hvordan digitalisering påvirker fartøydriften og cybersikkerheten på fartøy, noe som har skapt en viss avstand til den konkrete problemstillingen for bacheloroppgaven.

Vi er alle engasjerte i det operasjonelle elementet innenfor maritim næring, siden nautikkstudiet gir grunnlag for å kunne seile som dekksoffiserer. I en tidsalder med stadig digitalisering på forskjellige plan, blir også den maritime næringen stadig digitalisert, noe som vi trolig kommer til å observere i det kommende arbeidslivet, og synes derfor det er høyst interessant å studere problemstillingen angående hvordan den maritime næringen opplever at digitalisering påvirker fartøydriften og cybersikkerheten på fartøy. Det er derfor valid å bemerke at selv om forskergruppen har en viss avstand til den konkrete problemstillingen, så er vi likevel opptatt av disse sakene og at det derfor kan tenkes at vi uten hensikt vil kunne dra med noen grunntanker inn i forskningsprosjektet.

Temaene som forskningsprosjektets tittel «digitalisering knyttet til sikker drift og cybersikkerhet på fartøy» frembringer, med hensyn til henholdsvis temaene digitalisering, sikker fartøydrift og cybersikkerhet på fartøy har forskningsgruppen varierende faglige forkunnskaper om. Temaet sikker fartøydrift har vi grunnet nautikkstudiets egenart en god del faglige forkunnskaper om. Derimot har vi mindre faglige forkunnskaper når det gjelder temaene digitalisering og cybersikkerhet på fartøy.

## 3.3 KVALITATIVT FORSKNINGSINTERVJU

Steinar Kvale og Svend Brinkmann, som sitert i (Dalland, Metode og oppgaveskriving, 2020, s. 65) fremstiller det kvalitative forskningsintervjuet slik: «Hvis du vil vite hvordan folk oppfatter verden og livet sitt, hvorfor ikke spørre dem?» (Kvale & Brinkmann, 2015, s. 18). Dette belyser det som er mest sentralt og formålet med kvalitative forskningsintervju, nettopp det å innhente beskrivelser av intervjupersonen sin livsverden, for å kunne fortolke betydningen den har for intervjupersonen.

Dalland (2020, s. 67) utdyper videre at når temaet skal forstås ut fra intervjupersonens egne perspektiver, der det vektlegges meningen og fortolkningen av det som sies i intervjuet, tar Kvale og Brinkmann uttrykket livsverden et steg videre og kaller dette for et semistrukturert livsverdenintervju (2015, s. 46). Formuleringen semistrukturert betyr i denne sammenhengen at samtalen i intervjuet følger en intervjuguide med bestemte tema- og spørsmålsforslag (2015, s. 46). Med dette som grunnlag har vi funnet det mest formålstjenlig for denne studien å velge dybdeintervju som intervjuform.

Dybdeintervjuet er beskrevet som en intervjuform der intervjuet foregår som en planlagt og fleksibel samtale med formål om å anskaffe beskrivelser av intervjupersonens livsverden, med fokuset rettet mot meningen og fortolkningen av de fenomenene som blir fremstilt (Kvale & Brinkmann, 2015). Forskningsgruppen anser dette som en sikring for tilstedeværelsen av fleksibilitet til å gå nærmere inn på temaer som ikke kommer naturlig frem gjennom bruken av forskningsintervjuets intervjuguide, da forskningsintervjuene er planlagt gjennom utforming av to intervjuguider tilpasset intervjupersonenes yrke og stilling.

## 3.4 PLANLEGGING

Kvale og Brinkmann (2015) beskriver forskningsprosjektets planleggingsfase som avgjørende for å sikre at det videre arbeidet med oppgaven skal belyse problemstillingen best mulig. Derfor ble det i forkant av gjennomføring av intervjuene, vektlagt hvordan vi best kunne utforme intervjuguider for å hjelpe oss med å hente ut relevant data til oppgaven. Andre beslutninger angående forskningsprosjektets retning og utvikling ble gjort underveis i forskningsprosessen. I de neste delkapitlene blir det nøyere presentert hvordan studien har blitt strukturert.

Dette er første gang for alle medlemmene i forskningsgruppen at vi inntar rollene som forskere som innhenter egne data. For å sikre at forskningsetiske normer blir ivaretatt og at gruppens behandling av personopplysninger er i tråd med personvernregelverket, søkte vi til Norsk senter for forskningsdata (NSD). Forskningsprosjektet ble godkjent av NSD (Vedlegg 1) før vi

gjennomførte intervjuene, og i forkant av hvert intervju fikk intervjupersonene tilsendt et informasjonsskriv inneholdende mer detaljert informasjon om oppgaven i tillegg til en samtykkeerklæring der vedkommende hadde mulighet til å gi skriftlig samtykke ved eventuell deltakelse i forskningsprosjektet (Vedlegg 2).

### 3.4.1 UTVALGSBESKRIVELSE

Dalland (2020, s. 81) uttrykker at: «Det kvalitative intervjuet sikter mot å gå i dybden. Da kan ikke antallet intervjupersoner være for stort». Derfor bestemte forskningsgruppen at utvalget til det kvalitative forskningsprosjektet skulle begrenses til et antall på totalt fem intervjupersoner. Videre består utvalget av intervjupersoner som gruppen mener har særlig relevante kunnskaper og erfaringer knyttet til forskningsprosjektets tema for å kunne bidra med å belyse problemstillingen best mulig, og utvalget kan derfor beskrives som et strategisk utvalg (Dalland, 2020, s. 59). I tillegg består utvalget av intervjupersoner som hadde mulighet til å stille til intervju, og utvalget kan derfor også betegnes som et tilgjengelighetsutvalg (Malterud, 2017, p. 59)

Malterud (2017) forklarer at det i kvalitative studier er viktigere med innholdsrike data og kontekst enn representativitet og standardisering, og derfor har vurderinger om hvilke yrkesgrupper som skulle intervjues omhandlet hvilke yrkesgrupper som ville være mest adekvat for oppgavens tema. Derfor valgte vi å intervjue to dekksoffiserer, to rederiansatte og én ansatt i et maritimt teknologiselskap, der intensjonen med å intervjue disse spesifikke yrkesgruppene var at vi tenkte at denne samlingen av totalt fem intervjupersoner ville tilføre oppgaven størst grad av relevant informasjon med tilstrekkelig informasjonsstyrke, uten å måtte intervjue flere personer for å kunne danne et tilfredsstillende informasjonsgrunnlag for oppgaven. Forskningsgruppen vurderer derfor dette utvalget til å være et formålstjenlig utvalg for å kunne tilføre betydningsfulle synspunkt på problemstillingen. Videre, angående intervjupersonenes relevans for oppgaven, ble arbeidet deres knyttet til digitalisering, sikker fartøydrift og cybersikkerhet på fartøy vektlagt.

### 3.4.2 INTERVJUGUIDE

Intervjuguiden har som hensikt å lede intervjueren gjennom intervjuene ved å gjøre det lettere for intervjueren å huske temaene for samtalen og utformingen av den er derfor en fundamental del av et forskningsprosjekt (Dalland, 2020, s. 83). Dalland forklarer: «Å utarbeide en intervjuguide er samtidig å forberede seg faglig og mentalt til å møte intervjupersonen» (Dalland, 2020, s. 83).

Det ble utformet to intervjuguider tilpasset de to forskjellige gruppene av intervjupersoner, én for dekksoffiserer og rederiansatte og én for andre relevante aktører i maritim næring. Intervjuguidene er vedlagt i (Vedlegg 3). I utformingen av intervjuguidene ble det lagt vekt på at de to gruppene som skulle intervjues, skulle bli intervjuet etter samme overordnede temaer, med ulike spørsmålsforslag vinklet etter gruppen intervjupersoner. Vi valgte å gjøre det slik fordi vi ønsket å innhente forskjellige synspunkter med grunnlag i samme temaer for å gjøre det enklere å se sammenhenger i senere analyse av intervjuene. De to intervjuguidene ble videre utformet etter en felles målrettet struktur, introduksjon, hoveddel og oppsummering, og av hensynet til forskningsgruppens egenkompetanse ble spørsmålsforslagene hovedsakelig av en generell art med hovedfokus på å innhente opplevelser og meninger rundt forskningsprosjektets problemstilling.

Det er lett for at man ved å følge en strukturert intervjuguide bestående av tema og tilhørende spørsmålsforslag havner i en mer strukturert enn åpen intervjusituasjon. (Dalland, 2020, s. 83). «Jo åpnere intervjusituasjonen er, desto større er sjansen for å få spontane, levende og uventede svar. Jo mer strukturert intervjusituasjonen er, desto lettere er det å ferdigstrukturere og analysere intervjuet senere» (Dalland, 2020, s. 83). Forskningsgruppen tok derfor hensyn til disse faktorene ved utformingen av intervjuguidene i et forsøk på å skape en balanse mellom åpenhet og struktur i intervjusituasjonene, for å oppnå en best mulig gjennomførelse av intervjuene betinget forskningsgruppens ferdighetsnivå.

For å ytterligere øke sjansene for å få spontane, levende og uventede svar, ble det for majoriteten ikke sendt ut de fullstendige intervjuguidene til intervjupersonene på forhånd av intervjuene (Dalland, 2012). Når dette er nevnt, ble det i forkant av noen intervju, sendt ut et begrenset antall stikkord rundt temaene for intervjuet til intervjupersonene, da de uttrykte usikkerhet om at de ville kunne utveksle relevant informasjon. Her opptrådde forskningsgruppen forsiktig, og bedømmer derfor dette til å ha hatt ingen innflytelse på intervjusituasjonene, da stikkordene som ble utsendt var basert på allerede tilgjengelig informasjon til stede i forskningsprosjektets informasjonsskriv og samtykkeerklæring som de fikk tilsendt samtidig som stikkordene det ble bedt om.

## 3.5 GJENNOMFØRING AV INTERVJU

For å gjennomføre intervju ble intervjupersonene først kontaktet gjennom e-post. Forskningsgruppen formulerte en uniform og kort tekst som ble utsendt til alle eventuelle intervjupersoner ment til å informere om hvem vi er, hva forskningsprosjektet går ut på og

hvorfor de blir kontaktet. I tillegg ble det i samme e-posten, lagt ved et informasjonsskriv inneholdende mer detaljert informasjon om studien med mulighet om å gi skriftlig samtykke i en samtykkeerklæring. Vi valgte å formulere en uniform og kort tekst, i tillegg til å legge ved det essensielle informasjonsskrivet i e-postene, fordi vi håpte det ville gjøre det lettere for mottakerene å vurdere om de ville delta i forskningsprosjektet eller ikke ved første lesning av e-posten i tillegg til at vi synes det er viktig å legge et godt grunnlag for videre kontakt. Noen intervju ble arrangert gjennom videre samtaler på telefon etter først utsending av e-post.

Datainnsamlingen ble gjennomført over en periode på rundt seks uker, grunnet både medlemmene i forskningsgruppens og intervjupersonenes tilgjengelighet. Dette tidsrommet muliggjorde at vi kunne transkribere intervjuene, og gjennom evaluering av intervjuets kvalitet, forbedre intervjustilen og eventuelt gjøre endringer i intervjuguiden angående spørsmålsforslagene og andre mindre justeringer. Dette i et forsøk på å forbedre oss til de senere intervjuene og for å gjøre transkripsjonen tydeligere. Intervjuene ble gjennomført både ved fysiske møter og gjennom digitale møteløsninger, etter hva som passet intervjupersonene best, og alle tre studentene på forskningsgruppen var til stede på alle intervjuene.

Vi vurderte det som fordelaktig at vi fordelte klare roller for intervjusituasjonen, der én student hadde rollen som intervjuer og de to andre studentene hadde rollen som observatører. Før intervjuene begynte og vi startet lydopptak, forklarte vi forskningsprosjektet, hensikten med intervjuet, anonymitet og taushetsplikt og frivillig samtykke til å være med på lydopptak. Intervjuene ble deretter innledet med spørsmål om personalia, endog denne informasjonen ikke skal benyttes i noe stort omfang videre. Disse spørsmålene hadde bare til hensikt å tilrettelegge for en trygg og god atmosfære til den etterfølgende hoveddelen der vi ønsket å fremstille en mer flytende dialog med anledninger for lengre resonnement og eventuelle innspill som gikk utenfor intervjuguidenes opprinnelige struktur. Helt til slutt ble det stilt spørsmål med en kontrollerende hensikt for å kunne gå over om vi hadde forstått intervjupersonene riktig og om de eventuelt hadde mer de ville meddele. Intensjonen med en slik tilnærming til intervjusituasjonene var å forstørre sjansen for å få spontane, levende og uventede svar (Dalland, 2012).

Kvale og Brinkmann (2015) uttrykker at intervjuet skal gjennomføres på bakgrunn av en intervjuguide med en gjennomtenkt tilnærming. Alle studentene på gruppen fulgte derfor med på intervjuguiden for å holde oversikten gjennom intervjusituasjonen. Videre valgte vi som nevnt å gjennomføre intervjuene på en rigid måte der hver student hadde angitte roller for

intervjuet, der det bare var én intervjuer. Hensikten med dette var å prøve å gjøre intervjusituasjonen bedre for intervjupersonen, ved at intervjupersonen kunne fokusere på å forholde seg til bare én intervjuer gjennom den største delen av intervjuet. Observatørene noterte underveis i intervjusituasjonen, men ikke intervjueren, da dette mulig kunne flytte intervjuerens fokus bort ifra intervjupersonen. Deretter, når intervjuet nærmet seg slutten og vi hadde kommet til oppsummeringsdelen av intervjuguiden, åpnet intervjueren for at også observatørene kunne stille videre spørsmål til intervjupersonen om eventuelle poeng de hadde notert og som ikke hadde kommet opp gjennom intervjuet.

## 3.6 TRANSKRIPSJON

Transkripsjon er prosessen med å omgjøre lydopptak til skriftlig tekst, og for å legge til rette for analyse av datamaterialet, ble lydopptakene fra intervjuene transkriberte til skriftlige tekster. Malterud (2017) uttrykker at hensikten med å transkribere intervjuene, er at man gjennom å få lydopptakene konvertert til skriftlige tekster, bedre klarer å registrere det intervjupersonene hadde ønske om å meddele.

Transkripsjonen av intervjuene valgte forskningsgruppen å gjøre selv, både for å kunne lære om egen intervjustil og hvordan denne kunne forbedres før gjennomføringen av de neste intervjuene, og fordi at på denne måten kunne vi også ha en viss forståelse av de sosiale og emosjonelle aspektene til stede ved intervjusituasjonen (Kvale & Brinkmann, 2015). Transkripsjonen valgte vi å skrive hovedsakelig på bokmål da dette er et skriftspråk som hele forskningsgruppen behersker greit, der vi valgte å beholde noen ord og uttrykk på engelsk når dette var fordelaktig.

Det eksisterer flere forskjellige transkripsjonssystem å velge mellom tilpasset spekteret av elementer man velger å tilføye transkriberingen. Forskningsgruppen hadde ved alle intervjusituasjonene anledning til å vurdere intervjupersonenes helhetlige adferd angående ansiktsuttrykk og stemmebruk i tillegg til den selve verbale kommunikasjonen. Vi gjorde en beslutning om å benytte en enkel transkripsjonsstrategi og tok derfor bare med den selve verbale kommunikasjonen videre i analyseringsprosessen, der adferdsdetaljer som endringer i ansiktsuttrykk og stemmebruk ikke skulle være relevant for den videre analyseringsprosessen.

## 3.7 ANALYSE

Analyseringen av datamaterialet har blitt gjennomført ved bruk av metoden systematisk tekstkondensering beskrevet i Kirsti Malterud sin bok «Kvalitative forskningsmetoder for medisin og helsefag» fra 2017. Metoden systematisk tekstkondensering består av fire trinn, og

er regnet som en velegnet metode for tverrgående analyse av et datamateriale for utvikling av nye beskrivelser og begreper på bakgrunn av intervjupersonenes erfaringer, uavhengig av filosofisk perspektiv og metodevalg.

De fire trinnene i systematisk tekstkondensering er oppsatt etter rekkefølgen: foreløpige temaer, koding, kondensering og kategori. Det første trinnet, foreløpige temaer, går ut på å gjøre seg opp et helhetsinntrykk av datamaterialet. Det andre trinnet, koding, omhandler å identifisere meningsbærende enheter og samle disse i koder. Det tredje trinnet, kondensering, har til hensikt å sammenfatte disse kodene gjennom kondensering. Det fjerde trinnet, kategori, angår det å sortere de sammenfattede kodene i kategorier etter innhold (Malterud, 2017). Hvert av de fire trinnene i systematisk tekstkondensering vil bli nærmere beskrevet i de neste delkapitlene som tar for seg hvert enkelt trinn, der det for hvert enkelt trinn, vil bli forklart hvordan trinnet har bidratt i analyseprosessen.

Forskningsgruppens valg av å benytte denne analysemetoden argumenteres med at vi anser at denne analysemetoden vil best frembringe sammenhenger i datamaterialet i tillegg til at analysemetoden er beskrevet stegvis, noe som vi vurderer vil forenkle analyseprosessen for forskningsgruppen i rollen som forskere for første gang og dermed at datamaterialet får komme til sin rett. Malterud (2017, p. 100) uttrykker at det er en stor fordel å gjennomføre analysen av datamaterialet sammen med en annen forsker, og derfor valgte forskningsgruppen å gjennomføre analysen sammen med hele forskningsgruppen til stede.

### 3.7.1 FORELØPIGE TEMAER

Det første trinnet, foreløpige temaer, vektlegger helheten av intervjuenes innhold tyngre enn detaljene av intervjuenes innhold. Forskningsgruppen studerte derfor alle intervjutranskripsjonene i et forsøk på å oppnå en god kjennskap til innholdet i hele datamaterialet. Når forskningsgruppen hadde anskaffet et helhetsinntrykk over datamaterialets innhold, ble innholdet oppsummert ved at det ble utarbeidet foreløpige temaer basert på et fugleperspektivs inntrykk av innholdet i datamaterialet (Malterud, 2017, p. 99).

Utarbeidingen av de foreløpige temaene ble gjennomført i et nytt tekstdokument separert fra intervjutranskripsjonene for å beholde tekstdokumentene inneholdende intervjutranskripsjonene i urevidert tilstand. De foreløpige temaene ble deretter supplert med stikkord passende hvert foreløpige tema for å bidra til prosessen i å utforme en resulterende sammenhengende tekst. Malterud (2017, p. 100) forklarer at det er viktig å bemerke at disse foreløpige temaene bør ende opp med å være tilstrekkelig ulike fra temaene beskrevet i

intervjuguidene, da en for høy grad av likhet mellom disse kan antyde en minimal grad av kreativ og iterativ analyse der egen forforståelse påvirker analysen for mye. Forskningsgruppen sørget derfor for å tydelig skille mellom de foreløpige temaene og temaene fra intervjuguidene i et forsøk på å fremme en høyst mulig ryddig analyseringsprosess. Noen av de foreløpige temaene forskningsgruppen formulerte var: drivkrefter, hjelpemidler, risikoforståelse, kunnskapsgrunnlag og risikoappetitt.

### 3.7.2 KODING

Det andre trinnet, koding, innbefatter utskilling av relevant datamateriale fra irrelevant datamateriale, der bare datamaterialet forskningsgruppen har vurdert som relevant for å belyse forskningsprosjektets problemstilling beholdes. Malterud (2017) beskriver formålet med koding til å være identifisering av meningsbærende enheter. De foreløpige temaene oppsatt i første trinn ble her videreutviklet til kodegrupper, der kodingen foregikk ved at de meningsbærende enhetene ble plassert i kodegrupper som erstattet det som tidligere var foreløpige temaer.

Kodingen ble gjennomført i et nytt tekstdokument separert fra intervjutranskripsjonene for å sikre tilgang til ureviderte intervjutranskripsjoner. Forskningsgruppen hadde som formål å definere flest mulig meningsbærende enheter, samtidig som at omfanget av dette skulle være overkommelig innenfor studiens tidsfrist. I vurderingen av hvilke deler av datamaterialet som var av relevans, fokuserte forskningsgruppen på det innholdet som ville bidra til å belyse forskningsprosjektets problemstilling på en best mulig måte i tillegg til å kunne naturlig tilhøre de forskjellige kodegruppene. Innholdet som ikke ville bidra til å belyse problemstillingen og som ikke kunne naturlig tilhøre de forskjellige kodegruppene, ble vurdert som irrelevant og dermed forkastet for den videre analyseringsprosessen.

### 3.7.3 KONDENSERING

Det tredje trinnet, kondensering, har som formål å systematisk hente ut mening ved å kondensere innholdet i de meningsbærende enhetene som er kodet sammen til kondensat. Selve kondenseringen gjøres ved at materialet i kodegruppene deles inn i subkategorier, der det undersøkes hvilke aspekter av kodegruppen som kan beskrives av datamaterialet. Videre når kodegruppene er delt inn i subkategorier, skal teksten skrives om til et kondensat. Gullsitatene fra kodingen blir beholdt i jeg-form, men blir forkortet og omskrevet på en slik måte at meningen og essensen i de opphavlige sitatene blir bevart. Gullsitatene gjenspeiler hovedfunnene i forskningsprosjektet og består av utdrag fra kondensatene som forskningsgruppen anser best mulig belyser og oppsummerer innholdet (Malterud, 2017).

Malterud (2017, p. 105) anbefaler å benytte tre til fem kodegrupper, da det ved å benytte flere kodegrupper enn dette, blir vanskeligere å holde oversikten samtidig som det blir utfordrende å formulere tilstrekkelig robuste resultatpresentasjoner for hver kodegruppe. Forskningsgruppen endte derfor opp med å benytte tre kodegrupper, der vi anser antallet kodegrupper vi valgte å benytte som hensiktsmessig for bacheloroppgaven. Videre ble disse tre kodegruppene delt inn i totalt åtte subkategorier fordelt over kodegruppene.

Gjennom forskningsprosessen har forskningsprosjektets problemstilling blitt forandret noe i form av omskrivninger og presiseringer. Dette gjaldt forskjellige måter å uttrykke hvordan digitalisering i maritim næring har påvirket sikker fartøydrift og cybersikkerheten på fartøy. Vi anser ikke dette til å ha hatt noen merkbar innvirkning på forskningsprosjektets resultater, da dette bare omhandlet omskrivninger og presiseringer der vi fortsatt holdt oss innenfor temaet for bacheloroppgaven: «digitalisering knyttet til sikker drift og cybersikkerhet på fartøy».

### 3.7.4 KATEGORI

Det fjerde trinnet, kategori, omhandler at kondensatene fra forrige trinn skal sammenfattes til analytiske tekster, der dette blir grunnlaget for nye beskrivelser og begreper. De analytiske tekstene skal skrives i tredjeperson der målsetningen for forskningsgruppen er at de forskjellige intervjupersonene sine stemmer skal bli bevart så godt som mulig. Malterud (2017) uttrykker at dette blir gjort ved at forskningsgruppen gjennom å være lojal i gjenfortellingen av intervjupersonene sine uttalelser tar ansvar for at de blir tolket riktig. Etter utarbeidelsen av de analytiske tekstene, må det vurderes hvorvidt gullsitatene funnet i forrige trinn fortsatt er passende eller ikke, i tillegg til at kategoriene må få sine endelige navn (Malterud, 2017).

Forskningsgruppen brukte her kondensatene fra forrige trinn til å utarbeide en sammenfattet tekst for hver kodegruppe og subkategori og navnga resultatkategoriene hensiktsmessig. Gullsitatene som ble utpekt i forrige trinn ble deretter revurdert av forskningsgruppen angående hvorvidt de fortsatt var passende før de ble tilført hver subkategori.

Ved å benytte disse fire trinnene beskrevet i metoden systematisk tekstkondensering, har vi gjort kodegruppene om til kategorier som viser til studien sine funn. I tabellen under presenterer vi hvordan forskningsprosjektet sine kategorier ble utarbeidet ved å benytte denne metoden:

| | | |
|---|---|---|
| Trinn 1 | Foreløpige temaer | Etter å ha anskaffet en oversikt over datamaterialet, formulerte vi noen foreløpige temaer:<br>Drivkrefter og hjelpemidler |

| | | |
|---|---|---|
| Trinn 2 | Koding | Etter å ha formulert noen foreløpige temaer, identifiserte vi meningsbærende enheter som kunne passe under temaene drivkrefter og hjelpemidler.<br>Temaene henger sammen og danner en ny kodegruppe:<br>Opplevde drivkrefter med hensyn til sikker fartøydrift |
| Trinn 3 | Kondensering | Etter å ha kodet de meningsbærende enhetene til forskjellige kodegrupper, ble innholdet kondensert i tilhørende subkategorier |
| Trinn 4 | Kategori | Etter å ha kondensert innholdet i subkategorier, ble kondensatet av innholdet omskrevet til analytiske tekster. |

*Tabell 1: Kortfattet oversikt av analyseprosessen ved systematisk tekstkondensering*

## 3.8 FEILKILDER

Dalland (2020) forklarer at: «I hvilken grad resultatet er holdbart eller gyldig, avhenger av hvor godt vi er i stand til å gjøre rede for de valgene vi har tatt i løpet av prosessen, og hva de har hatt å bety for resultatet». Videre forklarer Dalland (2020) at man ved å gjøre rede for hvordan man har gjennomført forskningsprosjektet, der man forsøker å beskrive mulige feilkilder som kan ha påvirket forskningsprosjektets resultat, gjør at lesere av oppgaven har muligheten til å selv vurdere resultatenes pålitelighet.

Gjennom hele forskningsprosjektet har forskningsgruppen forsøkt å opptre så korrekt som mulig for å fremstille et mest mulig pålitelig resultat fra forskningen. Samtidig er forskningsgruppen klar over at feilkilder endog kan forekomme ved et forskningsprosjekt uten at man legger merke til det. Forskningsgruppen anser at siden det er første gang alle gruppemedlemmene inntar rollen som forskere, så kan den svært begrensede erfaringen angående hva som tilsier god forskning ha vært en feilkilde og bidratt med å styre resultatene i en ubestemt retning. Videre kan en feilkilde tenkes å være de avgrensningene vi har satt angående at intervjupersonene som har vært med i forskningsprosjektet er basert i Norge, der resultatene kanskje kunne blitt mer nyanserte om vi hadde hatt en bredere representasjon av forskjellige andre stater i tillegg til Norge. En annen feilkilde kan være at vår egen bakgrunn fra en maritim studieretning i et forskningsprosjekt rettet mot den maritime næringen kan tenkes å medbringe noe forforståelse som kan ha hatt innflytelse på hvordan vi tolker datamaterialet og dermed hvordan resultatene presenteres. Det kan også tenkes at intervjuguiden kan ha vært en feilkilde i den forstand at forskningsgruppens forforståelse kan ha påvirket spørsmålsforslagene i intervjuguiden og formet datamaterialet fra intervjuene og dermed resultatene.

# 4.0 RESULTAT

I dette kapittelet skal vi presentere resultatene av forskningsprosjektet. Resultatene er utarbeidet etter bidragene fra dekksoffiserene, de rederiansatte og den ansatte i det maritime teknologiselskapet. Analysen av datamaterialet i forskningsprosjektet resulterte i tre kategorier med tilhørende subkategorier som vises i tabellen under:

| Kategorier | Subkategorier |
|---|---|
| Drivkrefter knyttet til sikker fartøydrift | 1. Engasjement for digitalisering<br>2. Fordeler med digitalisering<br>3. Målsetninger for sikker fartøydrift |
| Utfordringer knyttet til cybersikkerhet | 1. Forhold til cybersikkerhet<br>2. Ulemper med digitalisering<br>3. Tiltak for bevaring av cybersikkerhet |
| Kompetansegrunnlag knyttet til bevaring av cybersikkerhet | 1. Prosedyrer og retningslinjer<br>2. Opplæring og øvelser |

*Tabell 2: Oversikt av resultatkategoriene*

Videre i dette kapittelet skal vi presentere kategoriene og subkategorier i egne delkapittel med tilhørende analytiske tekster og gullsitat.

## 4.1 DRIVKREFTER KNYTTET TIL SIKKER FARTØYDRIFT

Denne kategorien handler om drivkrefter knyttet til sikker fartøydrift, og hvordan den maritime næringen uttrykker at engasjement har aktualisert digitalisering, hvilke fordeler med digitalisering som oppleves og hvilke målsetninger for sikker fartøydrift som ønskes å oppnå gjennom digitalisering. Kategorien er tatt med i den hensikt at den skal redegjøre for årsakene til interessen den maritime næringen har for å bedrive digitalisering med hensyn til sikker fartøydrift.

### 4.1.1 ENGASJEMENT FOR DIGITALISERING

Dekksoffiserene forteller at de opplever digitalisering på fartøy som en tiltakende trend og gir uttrykk for at de er engasjerte i digitaliseringen av fartøydriften, da det har virket hensiktsmessig for en sikker fartøydrift, med forbedring og forenkling av mange prosesser knyttet til deres arbeid om bord på fartøyet. Den ene dekksoffiseren forklarte at dette gjaldt eksempelvis automatisering av prosesser som tidligere innebar manuell innføring av informasjon, der man gjennom automatisering har oppnådd at informasjonen automatisk innføres og blir nøyaktigere enn det som tidligere var oppnåelig. Den andre dekksoffiseren

anser ikke seg selv som noen motstander mot digitalisering på fartøy, men opplever at noen digitaliserte prosesser kan være vanskelig å forstå seg på, men forteller at når man forstår logikken i prosessene så ser man nytten digitaliseringen har.

De rederiansatte uttrykte at de har vært nysgjerrige på digitalisering av fartøydriften i en lengre periode, og forteller at digitalisering av fartøydriften oppleves å ha mange fordeler som bidrar til å oppnå målsetningene deres om en sikker fartøydrift. De rederiansatte forklarer videre at det derfor er et pågående engasjement angående digitalisering på fartøy ved implementering av flere digitale løsninger, og nevner digitale sjekklister og uthenting av sanntidsinformasjon angående drivstofforbruk som eksempel på dette. Den ene rederiansatte forteller at sjøsiden og landsiden har ulike informasjonsinteresser, der sjøsiden trenger taktisk informasjon for å gjøre taktiske valg og landsiden trenger strategisk informasjon for å gjøre strategiske valg, og at det dermed er forskjellige innfallsvinkler til engasjementet for digitalisering på fartøy.

Den ansatte i det maritime teknologiselskapet forteller at det oppleves å være et engasjement for å bedrive digitalisering på fartøy, og nevner at rederier undersøker hvordan de gjennom digitalisering av fartøydriften kan bedrive sikker fartøydrift innenfor regelverket med et lavere antall sjøfolk om bord, som et eksempel på dette. Den ansatte i det maritime teknologiselskapet uttrykker videre at digitalisering på fartøy er en sentral trend i denne samtiden som trolig vil tilta i styrke siden rederier ser nyttene det kan medføre for fartøydriften, blant annet ved positiv endring av kostnadsbasen. Den ansatte i det maritime teknologiselskapet tenker derfor at digitalisering på fartøy vil prege fartøydriften fremover.

Gullsitat:

*Jeg synes det gjør hverdagen mye enklere, mye enklere å få oversikt og mye lettere for meg i min stilling å utføre mitt arbeid. Det er nå mye enklere, nesten sånn at jeg lurer på hva jeg glemmer, fordi at det har blitt så mye enklere enn det var før i tiden.*

### 4.1.2 FORDELER MED DIGITALISERING

Dekksoffiserene uttrykker at de opplevde fordelene ved digitalisering på fartøy omhandler at prosesser effektiviseres og forenkles, noe som medfører at det blir enklere å holde oversikten og fatte gode beslutninger for en sikker fartøydrift. Den ene dekksoffiseren opplever at digitalisering på fartøy tillater at man kan vie et større fokus på de oppgavene man anser å være viktigst gjennom automatisering av rutineoppgaver i tillegg til at man i større grad kan bruke frivaktene hensiktsmessig slik at man har bedre forutsetninger til å bedrive en sikker fartøydrift. Dekksoffiseren forklarer også at digitalisering på fartøy medfører bedre argumenter for å

bestemme vedlikeholdsintervaller på fartøykomponenter, der man gjennom innsamling av informasjon om fartøykomponenters faktiske helsestatus kan basere vedlikeholdsintervaller på dette i stedet for at vedlikeholdsintervaller er tidsbaserte. Den andre dekksoffiseren forklarer at det gjennom digitalisering på fartøy har blitt enklere å motta hjelp til å utbedre feil ved digitale løsninger på fartøyet, der man kan motta hjelp gjennom fjerntilgang til fartøyet fra land.

De rederiansatte forteller at de opplevde fordelene ved digitalisering på fartøy angår at det fremstiller en bedre oversikt over hvordan de kan fremme sikker fartøydrift gjennom sammenstilling av informasjon fra flere og nøyaktigere kilder. Den ene rederiansatte forteller at digitalisering på fartøy setter de i en posisjon til å studere flere typer informasjon på tvers av hverandre, slik at de kan utvide de operasjonelle kunnskapene om fartøydriften angående forskjellige tiltak sine påvirkninger og dermed gjøre beslutninger basert på et bedre informasjonsgrunnlag, og uttrykker videre at digitalisering på fartøy har tilrettelagt for å anskaffe verdifulle kunnskaper for å operere fartøy sikrere og mer økonomisk. Den andre rederiansatte forteller at digitalisering på fartøy oppleves som nyttig da det bidrar med å knytte fartøy og rederikontor nærmere ved at man gjennom digitale løsninger kan følge med på fartøydriften fra landsiden og eventuelt foreslå forandringer. Den rederiansatte poengterer også at gjennom digitalisering på fartøy har det blitt enklere å motta hjelp til å utbedre feil ved digitale løsninger på fartøyet ved fjerntilgang til fartøyet fra land.

Den ansatte i det maritime teknologiselskapet forklarer at digitalisering av fartøydriften gir fordeler for fartøydriften ved å muliggjøre at de gjennom digitale løsninger for innsamling av informasjon på fartøy kan styrke forståelsen av fartøyflåtens driftsprofiler og følgelig forståelsen angående påvirkninger eventuelle forandringer har. Den ansatte i det maritime teknologiselskapet opplever også at fordelene ved digitalisering på fartøy er at man kan knytte sjøsiden og landsiden tettere ved at landsiden gjennom digitale løsninger har fjerntilgang til enkelte fartøykomponenter fra landsiden. Den ansatte i det maritime teknologiselskapet forteller videre at digitalisering på fartøy åpner for at fartøy kan motta fjernstøtte for å utbedre problemer gjennom fjerntilgang til digitale løsninger fra landsiden.

Dekksoffiserene, de rederiansatte og den ansatte i det maritime teknologiselskapet uttrykker at digitalisering på fartøy, med hensyn til sikker fartøydrift og cybersikkerheten på fartøy, totalt sett oppleves som noe positivt. Dekksoffiserene forteller at fordelene for sikker fartøydrift som kommer i kjølvannet av digitaliseringen på fartøy oppleves å veie opp for de eventuelle

risikoene som finnes for cybersikkerheten på fartøy. De rederiansatte forklarer at digitalisering på fartøy uten tvil medfører flere gevinster enn utfordringer med hensyn til henholdsvis sikker fartøydrift og cybersikkerheten på fartøy. Den ansatte i det maritime teknologiselskapet opplever at digitalisering på fartøy for de fleste rederier anses å gagne sikker fartøydrift, da de fleste rederier samtidig har tilfredsstillende prosesser for bevaring av cybersikkerheten på fartøy.

Gullsitat:

*Det gir uten tvil et positivt utfall av å digitalisere, det er ikke noe … altså den ballen klarer du ikke å stoppe. Du er bare nødt til å henge med på det hvis du har tenkt å være med videre fordi kraften i all informasjonen er så stor at det ikke er et alternativ å la være.*

### 4.1.3 MÅLSETNINGER FOR SIKKER FARTØYDRIFT

Dekksoffiserene opplever at rederiene er proaktive når det gjelder digitalisering på fartøy, og forteller at rederiene har tilrettelagt for implementering og bruk av flere digitale løsninger på en hensiktsmessig måte for å oppnå målsetningen om sikker fartøydrift. Dekksoffiserene gir videre uttrykk for at sjøsiden og landsiden må bidra på hver sin front ved digitalisering av fartøydriften for at digitaliseringen skal ha tiltenkt effekt og dermed oppnå målsetningene for fartøydriften. Dekksoffiserene opplever at begrunnet rederienes størrelse, så er rederiene avhengige av at implementering av nye digitale løsninger på fartøy foregår på en god måte for å oppnå målsetningene for fartøydriften. Dekksoffiserene forklarer videre at dette omhandler tilfredsstillende oppfølging av sjøfolkene, slik at de har den opplæringen som trengs for å kunne anvende de nye digitale løsningene som tiltenkt. Dekksoffiserene opplever at digitaliseringen på fartøy har kommet ganske langt og at det nå for tiden derfor eksisterer mange flere muligheter enn før angående bruk av digitale løsninger for å oppnå rederienes målsetninger for fartøydriften.

De rederiansatte uttrykker at de er opptatte av sikker fartøydrift, og at de har kontinuerlige målsetninger om at fartøyene skal operere sikkert med minst mulig ressursbruk gjennom digitalisering på fartøy. De rederiansatte forteller videre at det er et felles ansvar mellom sjøsiden og landsiden for at målsetninger for fartøydriften gjennom digitalisering skal bli oppfylt, og forklarer at man er avhengige av gode bidrag fra begge fronter. Den ene rederiansatte forteller at de har observert kontrakter med eksplisitte krav til at fartøyet på kontrakten måtte ha digitale løsninger for overføring av informasjon om drivstofforbruk til kontraktøren, slik at de kunne ha oversikt over fartøyets drivstofforbruk på kontrakten, og

uttrykker at dette har forsterket målsetningen deres om digitalisering på fartøy. Den andre rederiansatte uttrykker ikke at målsetningen deres angående digitalisering på fartøy har blitt forsterket, og forklarer dette med at de er fornøyde med avkastningene de allerede opplever av det gjeldende omfanget av digitalisering.

Den ansatte i det maritime teknologiselskapet forklarer at de er interessert i digitalisering på fartøy, og at deres målsetninger innenfor fartøydrift hovedsakelig omhandler det operative aspektet. Den ansatte i det maritime teknologiselskapet opplever videre at hvorvidt ansvaret for at målsetninger for fartøydrift gjennom digitalisering skal bli oppfylt ligger på sjøsiden eller landsiden, kommer an på hvem digitaliseringen og følgelig de digitale løsningene som benyttes angår. Den ansatte i det maritime teknologiselskapet tenker at alle målsetninger for fartøydriften gjennom digitalisering enten omhandler tilfredsstillelse av regulatoriske krav eller økning av profitt for rederier, og forklarer at de samarbeider med rederier for at de skal nå disse målsetningene.

Gullsitat:

*De fleste er veldig positive, og vi jobber jo sammen da, om å oppnå de målsetninger vi har for fartøydriften angående blant annet det å redusere forskjellig forbruk. Så det er ikke slik at de om bord føler seg overvåket og at vi skal sitte her og pirke på dem, det har jeg ikke følelsen av da. Samtidig er de veldig flinke å komme med spørsmål og forslag, ikke minst hvis det er saker de om bord kan gjøre litt annerledes og sånn.*

## 4.2 UTFORDRINGER KNYTTET TIL CYBERSIKKERHET

Denne kategorien handler om utfordringer knyttet til cybersikkerhet, og hvordan den maritime næringen uttrykker at forholdet deres er til cybersikkerhet, hvilke ulemper med digitalisering som oppleves og hvilke tiltak for å bevare cybersikkerheten som gjøres.

### 4.2.1 FORHOLD TIL CYBERSIKKERHET

Dekksoffiserene uttrykker at de har et fokus på cybersikkerheten på fartøy, og forteller at de aldri har registrert noen cyberangrep mot fartøy. Dekksoffiserene opplever videre at hvor god cybersikkerheten er på fartøy, er avhengig hver enkel person i mannskapet sin adferd når de er tilkoblet fartøyets internett. Den ene dekksoffiseren opplever at cybersikkerheten på fartøy i 2022 er god, men tenker videre at det kan være variasjoner mellom fartøy i et og samme rederi angående hvor seriøst man tar cybersikkerhet på fartøy.

Dekksoffiseren tenker at det må skje et tydelig brudd på cybersikkerheten på fartøy som merkes av hele mannskapet før enkelte våkner og at cybersikkerhet på fartøy dermed blir tatt seriøst selv om det er beskrevet i sikkerhetsstyringssystemet. Dekksoffiseren tenker videre at grunnen til at cybersikkerhet ikke blir tatt like seriøst av alle sjøfolk, er at de rett og slett ikke har et reelt forhold til hendelser angående cybersikkerhet sammenlignet med andre hendelser på fartøy. Den andre dekksoffiseren forteller om en usikkerhet angående hvor god cybersikkerheten på fartøy i 2022 er, men tenker at brudd på cybersikkerheten på fartøy oftere skyldes menneskelige feilvurderinger enn svakheter ved de teknologiske sikkerhetsbarrierene på fartøy.

De rederiansatte forteller at cybersikkerhet har vært et kontinuerlig fokusområde for de gjennom de siste årene. De rederiansatte opplever at det alltid må være en balanse mellom funksjonalitet og cybersikkerhet ved digitalisering på fartøy. De rederiansatte forklarer videre at om man ønsker fullstendig cybersikkerhet så vil dette ofte medføre tilnærmet null funksjonalitet. De rederiansatte forteller også at de bestandig mottar informasjon fra fagkyndige innen cybersikkerhet angående det gjeldende globale trusselbildet for cybersikkerheten på fartøy.

Den ene rederiansatte uttrykker at cybersikkerheten på fartøy i 2022 er varierende, men at det oppleves at de har god cybersikkerhet på de viktige områdene. Den rederiansatte har videre en opplevelse av at de gjør de riktige tiltakene for å opprettholde cybersikkerheten på fartøy, men tenker at det er en illusjon at man kan sikre seg fullstendig mot cyberangrep mot fartøy. Den andre rederiansatte opplever at cybersikkerheten på fartøy i 2022 er grei, og forteller videre at det tenkes at trusselbildet for cybersikkerheten er ganske likt mellom fartøy og rederikontor. Den rederiansatte forteller også at det oppleves at noen fartsområder påberoper en bedre cybersikkerhet.

Den ansatte i det maritime teknologiselskapet opplever at cybersikkerheten på fartøy i 2022 er veldig varierende, men at trenden viser at det er klart økende bevissthet angående cybersikkerhet. Den ansatte i det maritime teknologiselskapet forklarer at rederier har ulike sikkerhetsbehov, da de har ulike elementer som de ønsker å beskytte og at rederier derfor trenger passende sikkerhetsprofiler for å hensiktsmessig kunne mitigere eventuelle trusler for cybersikkerheten ved operasjonene de utfører. Den ansatte i det maritime teknologiselskapet tenker videre at det er viktig at rederier forstår hvordan de kan håndtere eventuelle risikoer for cybersikkerheten på fartøy som følger digitalisering av fartøydriften, og begrunner dette med

at tidsrommet fra en sårbarhet ved cybersikkerheten på fartøy blir oppdaget av en som akter å utføre cyberangrep til at cyberangrepet deretter utføres, ofte er smalt.

Gullsitat:

*Jeg tror du er nødt til å kjenne litt på det før du på en måte kan … at det føles reelt da. Sånn som andre typer hendelser som eksempelvis brann, eller hva det måtte være, det har jo skjedd og det er jo statistikker på sånn og sånn, men for cyberangrep er det jo lite av.*

### 4.2.2 ULEMPER MED DIGITALISERING

Dekksoffiserene forteller at en ulempene de registrerer ved digitalisering på fartøy er at noen sjøfolk opplever at det medfører en overvåkning av deres handlinger på fartøy, og at noen sjøfolk oppfatter digitalisering på fartøy som en utvikling som de av ulike grunner ikke er tilhengere av. Den ene dekksoffiseren tenker at et problem med digitalisering på fartøy er om det danner grunnlag for usunn konkurranse mellom to relativt like fartøy i samme rederi, der fartøyet som presterer dårligst av de to eventuelt begynner å ta unødvendige sjanser eller snarveier for å danne et bedre bilde av fartøydriften enn det som er realiteten for å kunne måle seg med det andre fartøyet.

Dekksoffiseren forteller også at et problem med digitalisering på fartøy er at cybersikkerhet på fartøy ikke blir tatt så seriøst som det kanskje burde i denne samtiden. Dekksoffiseren har videre også registrert at noen sjøfolk er skeptiske til at stadig flere fartøykomponenter skal være tilkoblet internett da dette tenkes å medføre problemer for sikker fartøydrift om fartøyet skulle bli utsatt for cyberangrep. Den andre dekksoffiseren uttrykker at digitalisering på fartøy noen ganger oppleves å medføre ulemper i form av digitale løsninger som er vanskelige å bruke, der de tenker at de like greit kunne klart seg med enklere løsninger.

Den ene rederiansatte uttrykker at ulempen de opplever ved digitalisering på fartøy er at noen sjøfolk kan føle seg overvåket i deres handlinger på fartøy. Den andre rederiansatte uttrykker at digitalisering på fartøy medfører en ulempe ved at de i større grad blir avhengige av eksterne ressurser med fullverdig kompetanse innen cybersikkerhet for å bevare cybersikkerheten på fartøy når det bedrives digitalisering av fartøydriften der fartøy kan bli mer sårbare for cyberangrep.

Den ansatte i det maritime teknologiselskapet forteller at digitalisering på fartøy kan medføre ulemper i form av at fartøy kan bli mer sårbare for cyberangrep og at investeringer i ganske

dyre digitale løsninger for fartøy kombinert med begrensninger i båndbredde på fartøy for å bruke de digitale løsningene kan gi dårligere uttelling av investeringene enn forventet.

Gullsitat:

*Det er jo ikke så skyhøye marginer i maritim sektor, så det er jo, alt må jo forsvares fra et kost-nytte type ståsted. Så ta sånn med drivstoffoptimalisering og sånne ting er jo typisk ting som er opplagt. Du ser jo det på operative kostnader, du ser det på bunnlinja med en gang. Mens andre ting som du ikke ser på bunnlinja, det er ikke så interessant.*

### 4.2.3 TILTAK FOR BEVARING AV CYBERSIKKERHET

Dekksoffiserene uttrykker at tiltakene som gjøres på fartøy for å bevare cybersikkerheten på fartøy er at mannskapet blir bedt om å være bevisste i sine handlinger tilkoblet fartøyets internett. Den ene dekksoffiseren uttrykker at de stoler på at tiltakene for bevaring av cybersikkerheten på fartøy innført av de som har ekspertise angående cybersikkerhet fungerer, men at de likevel ønsker å selv gjøre en innsats. Dekksoffiseren forteller videre at det derfor som et forebyggende tiltak stadig tas opp på fartøyet at man skal være kritisk til mistenksomme e-poster som kan inneholde farlige lenker ment til å utføre cyberangrep når man er tilkoblet fartøyets internett. Den andre dekksoffiseren forteller at de gjennom bevisstgjørende prosesser rundt cybersikkerhet på fartøy har innført flere forebyggende tiltak mot cyberangrep. Dekksoffiseren forklarer videre at dette blant annet omhandler å bevisst skille mellom bruken av private datamaskiner tilkoblet fartøyets internett og datamaskiner direkte tilkoblet fartøyets digitale løsninger.

De rederiansatte forteller at de kontinuerlig prøver å innføre tiltak som gjør de motstandsdyktige mot de gjeldende truslene som finnes for cybersikkerheten på fartøy. De rederiansatte forklarer videre at et tiltak de har for å bevare cybersikkerheten på fartøy er at de har en praksis om at visse fartøykomponenter er frakoblet internett som standard, der fartøykomponentene bare tilkobles internett ved behov.

De rederiansatte tenker videre at dette tiltaket har gjort fartøy mindre sårbare for cyberangrep, da det ikke foreligger en kontinuerlig tilgang til fartøykomponentene ved at de ikke alltid er tilkoblet internett. Den ene rederiansatte uttrykker å ha en opplevelse av at mannskapet utgjør den største risikoen for cybersikkerheten på fartøy, og forklarer derfor at den største andelen av tiltak for å bevare cybersikkerheten på fartøy har angått å øke sjøfolkenes bevissthet angående cybersikkerhet. Den rederiansatte forteller videre at de også har iverksatt tekniske løsninger og utarbeidet en generisk risikovurdering av cybersikkerheten på fartøy ment for å

videre tilpasses hvert enkelt fartøy som tiltak for å bevare cybersikkerheten på fartøy. Den andre rederiansatte forteller at de som et tiltak for å bevare cybersikkerheten på fartøy, har utsendt informasjon til fartøy om gode rutiner for bevaring av cybersikkerheten på fartøy, og nevner at dette gjelder blant annet ganske grunnleggende saker som at man ikke skal tilkoble private minnepinner til fartøyets digitale løsninger. Den rederiansatte forteller videre at de også har som et tiltak at ansatte i rederiet oppfordres til å melde ifra ved mottak av mistenksomme e-poster, slik at rederiet er opplyste om dette i tilfelle de skulle motta samme e-postene.

Den ansatte i det maritime teknologiselskapet tenker at det er et felles ansvar mellom sjøsiden og landsiden i et rederi at tiltak i form av at cybersikkerhet på fartøy blir tatt opp som en del av sikkerhetsrutinene på fartøyet. Den ansatte i det maritime teknologiselskapet forklarer videre at et sentralt tiltak for å bevare cybersikkerheten på fartøy, er at man eliminerer potensielle angrepsvektorer for de digitale løsningene på fartøyet, slik at man reduserer de digitale løsningenes angrepsoverflater. Den ansatte i det maritime teknologiselskapet uttrykker også at et tiltak for bevaring av cybersikkerheten på fartøy er å ikke koble sammen IT og OT løsninger, der de i stedet sørges for å segmenteres tydelig med effektive og verifiserte barrierer.

Gullsitat:

*Ta DP-en for eksempel, så er det mulig å koble opp DP-en til internett, men som basis så er ledningen dreiet ut hos oss. Så man må anskaffe en arbeidstillatelse om man skal koble DP-en til internett for å gjøre vedlikehold. Så da sikrer vi på en måte at vi er i en god posisjon der det ikke kan skje noen særlige hendelser i det vi holder på med, før vi kobler oss til DP-en og utfører vedlikeholdet med servicefolkene fra land og frakobler DP-en fra internett igjen. På den måten minimerer du muligheten for å få ting over.*

## 4.3 KOMPETANSEGRUNNLAG KNYTTET TIL BEVARING AV CYBERSIKKERHET

Denne kategorien handler om kompetansegrunnlag knyttet til bevaring av cybersikkerhet, og hvordan den maritime næringen beskriver at prosedyrer og retningslinjer har veiledet dem angående cybersikkerhet og hvilken opplæring og øvelser angående cybersikkerhet de har gjennomført.

### 4.3.1 PROSEDYRER OG RETNINGSLINJER

Den ene dekksoffiseren forteller at rederiet har utarbeidet prosedyrer angående cybersikkerhet på fartøy. Dekksoffiseren forklarer videre at rederiet har over en lengre periode vært opptatte av cybersikkerhet på fartøy, men at fokuset i rederiet angående dette økte etter at IMO-kravet

om å innføre cybersikkerhet som en del av sikkerhetsstyringssystemet kom 1. januar 2021. Den andre dekksoffiseren forteller at rederiet ikke har utarbeidet prosedyrer angående cybersikkerhet på fartøy. Dekksoffiseren uttrykker at rederiet derimot har utarbeidet en instruksjonsmanual for cybersikkerheten på fartøy, og at rederiet har utsendt retningslinjer til fartøy angående cybersikkerhet på fartøy. Dekksoffiseren opplever likevel at instruksjonsmanualen ikke er helt implementert enda, da den ikke har blitt fulgt opp skikkelig.

De rederiansatte forteller at de har utarbeidet detaljerte prosedyrer og retningslinjer som angår den praktiske delen av cybersikkerhet på fartøy. Den ene rederiansatte uttrykker at de hadde prosedyrer for å bevare cybersikkerheten på fartøy allerede før IMO-kravet om å innføre cybersikkerhet som en del av sikkerhetsstyringssystemet kom 1. januar 2021, der de etter at IMO-kravet kom, også gjennomførte risikovurderinger angående cybersikkerheten på fartøy. Den andre rederiansatte forteller at prosedyren deres for å bevare cybersikkerhet på fartøy hovedsakelig ble utarbeidet av rederiet selv, men forklarer at de underveis også gjennomgikk prosedyren med eksperter innen cybersikkerhet på fartøy.

Den ansatte i det maritime teknologiselskapet uttrykker at innholdet i IMO-kravet om å innføre cybersikkerhet som en del av sikkerhetsstyringssystemet som kom 1. januar 2021, kan tolkes vidt forskjellig mellom rederier. Den ansatte i det maritime teknologiselskapet forteller videre at rederier derfor har ulike innfallsvinkler når de utarbeider prosedyrer som er ment for å bevare cybersikkerheten på fartøy. Den ansatte i det maritime teknologiselskapet tenker at uavhengig av innfallsvinkler for utarbeiding av prosedyrer for å opprettholde cybersikkerheten på fartøy, så er det viktigste at disse prosedyrene blir forstått riktig av sjøfolkene slik at prosedyrene kan virke etter tiltenkt hensikt.

Gullsitat:

*Jeg tror nok at det skapte et litt større fokus på cybersikkerhet på fartøy etter at disse prosedyrene kom i vårt sikkerhetsstyringssystem, samtidig som det naturlig nok, rett etter at du har tatt et sånt kurs, så er du kanskje veldig fokusert på det.*

### 4.3.2 OPPLÆRING OG ØVELSER

Dekksoffiserene forteller at de har fått opplæring og gjennomgått øvelser knyttet til cybersikkerhet på fartøy. Den ene dekksoffiseren uttrykker at det som er utslagsgivende for en sikker fartøydrift, med hensyn til blant annet cybersikkerhet på fartøy, først og fremst er god opplæring. Dekksoffiseren forteller videre at de har hatt e-kurs og øvelser angående cybersikkerhet på fartøy. Dekksoffiseren opplever dessverre at disse e-kursene og øvelsene

ofte blir litt for overfladiske. Dekksoffiseren uttrykker videre at selv om slike e-kurs og øvelser er en god start, så savnes det noe mer håndfast slik at hendelser knyttet til cybersikkerhet skal kjennes reelt. Dekksoffiseren forteller at man i stedet burde gjennomføre uanmeldt sak-trening angående cybersikkerhet på fartøy med støtte fra fagkyndige innen cybersikkerhet, der sjøfolk får øve på forskjellige scenarier omhandlende at fartøyet blir utsatt for cyberangrep. Dekksoffiseren legger til at dette vil kunne istandgjøre sjøfolk til å oppdage cyberangrep på et tidligere stadie, slik at cyberangrep ikke klarer å påføre noen skader mot fartøyet.

De rederiansatte forteller at de har hatt opplæring på cybersikkerhet og at det arrangeres opplæring i form av øvelser på fartøyene angående cybersikkerhet på fartøy. Den ene rederiansatte forklarer at opplæringen i cybersikkerhet har angått å bevisstgjøre de rundt tilkobling til forskjellige nettverk og deres handlinger på internett med hensyn til å være forsiktige med mistenksomme e-poster. Den andre rederiansatte poengterer at det oppleves at sjøfolkene er ganske godt drillet i det å bevare cybersikkerheten på fartøy. Den rederiansatte uttrykker videre at for å opprettholde cybersikkerheten på fartøy, så blir det blant annet avklart hvilke digitale løsninger som utgjør en utpreget risiko for cybersikkerheten på fartøyet og hvem som skal varsles ved eventuelle cyberangrep. Den rederiansatte forteller videre at etter øvelsene innen cybersikkerhet på fartøy er over, blir det utarbeidet øvelsesrapporter på fartøyene, der det blant annet blir notert eventuelle forslag til forbedring av øvelsene.

Den ansatte i det maritime teknologiselskapet forteller at det er viktig at opplæringen og øvelsene innen cybersikkerhet på fartøy gjenspeiler det bestemte behovet for cybersikkerhet som følge av digitaliseringen av fartøydriften, der opplæring og øvelser må være relevante for å virke forebyggende mot cyberangrep på fartøy og for å kunne forberede sjøfolk på å håndtere eventuelle brudd på cybersikkerheten på fartøyet. Den ansatte i det maritime teknologiselskapet forklarer videre at de fleste sjøfolk og rederiansatte har en helt annen bakgrunn enn fagkyndige innen cybersikkerhet, og at kompetansegrunnlaget i forkant av opplæring og øvelser innenfor cybersikkerhet på fartøy dermed er annerledes.

Gullsitat:

*Det kom ganske tidlig fra rederiet … både det med øvelser, prosedyrer og et sånt e-kurs da. Men du må på en måte ha noe litt mer håndfast … en knagg å henge ting på før det skal kjennes reelt, og vi kan jo si mye om e-kurs … men det blir dessverre litt tynt.*

# 5.0 DRØFTING

I dette kapittelet skal de presenterte resultatene fra forrige kapittelet drøftes opp mot problemstillingen og det teoretiske grunnlaget for oppgaven. Kapittelet tar for seg subkategoriene presentert i forrige kapittel. Deretter blir kapittelet avsluttet med en oppsummering.

## 5.1 ENGASJEMENT FOR DIGITALISERING

I Digital21-rapporten uttrykkes det at den maritime næringen er en av de ledende bransjene i Norge angående å utnytte mulighetene som digitalisering medfører, der den norske maritime næringen også er i toppsjiktet internasjonalt på mange områder grunnet den spesielle kombinasjonen av forskjellige maritime aktører (Digital21, 2018).

Alle de intervjuede uttrykker at det er et pågående engasjement for digitalisering på fartøy, da det har forbedret og forenklet mange prosesser knyttet til sikker fartøydrift både fra sjø- og landsiden av et rederi gjennom implementering av digitale løsninger. Det uttrykkes videre av alle intervjuede at prosesser knyttet til sikker fartøydrift har blitt forbedret og forenklet ved digitalisering på fartøy og at dette derfor har vært en drivkraft for digitalisering.

Det kan argumenteres for at sikker fartøydrift gjennom digitalisering på fartøy må som en base involvere kompetente sjøfolk, samtidig som rederier må være risikovillige for å investere i digitalisering. I tillegg trengs det skipsutstyrsbedrifter som kan frembringe formålstjenlige digitale løsninger. Disse faktorene kan tale for at den spesielle sammensetningen som den norske maritime næringen representerer, sammen har fremstilt engasjementet for digitalisering på fartøy.

Videre kan det tenkes at engasjementet for digitalisering på fartøy i den maritime næringen har noe bedre fotfeste i Norge enn andre land begrunnet den norske maritime næringens posisjon internasjonalt. Dette omhandler evnen den norske maritime næringen har til å ta i bruk forskjellige muligheter for digitalisering, der kanskje andre land hadde vært mindre interesserte i å utforske mulighetene ved digitalisering. Dette kan videre tenkes å omhandle forskjellig økonomisk satsing mellom land, der Norge i forhold til mange andre land lenge har satset kraftig på utvikling innenfor den maritime næringen for å kunne konkurrere med andre maritime aktører på et globalt plan.

I Fafo-rapporten forklares det at autonome og førerløse fartøy ikke er det mest aktuelle for informantene i rapporten, der det uttrykkes videre at de i stedet er opptatt av hvordan

kombinasjoner av ny teknologi og økende automatisering gir muligheter for å behandle store mengder informasjon og samtidig gi en rekke optimaliseringsgevinster. Disse fordelene er knyttet til drift, innovasjon og nye forretningsmodeller (Andersen, Bjørnset, & Rogstad, 2019).

Den ene dekksoffiseren nevnte at man gjennom automatisering av tidligere menneskehåndterte manuelle prosesser har gjort enkelte prosesser nøyaktigere enn tidligere oppnåelig. Basert på dette utsagnet kan det tenkes at en part av engasjementet for digitalisering på fartøy omhandler å redusere menneskelig påvirkning av informasjonsgrunnlaget. På grunn av at dette informasjonsgrunnlaget skal fremstille statistikker for fartøydriften, vil følgelig nytteverdien av å innsamle store mengder informasjon være avhengig av hvorvidt informasjonen er nøyaktig nok til å kunne gi et riktig bilde av fartøydriften.

Videre kan det også tenkes at automatisering av rutinemessige oppgaver knyttet til fartøydriften har vært formålstjenlig for sikker fartøydrift ved å tilrettelegge for en bedre oversikt, slik at man i større grad kan fokusere på hva som skal til for å kunne bedrive en sikker fartøydrift. Endog det tales for å redusere menneskelig påvirkning ved fartøydriften, er det ingenting som antyder at det ønskes å fjerne det viktige menneskelige bidraget på fartøy angående det operasjonelle, og dette kan kanskje bety at den maritime næringen har en forståelse av at det menneskelige bidraget er essensielt for å kunne bedrive en sikker fartøydrift.

Rapporten fra Fafo forklarer at digitalisering representerer et stort potensial for den maritime næringen, men samtidig oppgis det at en større del av maritim næring mangler digital kompetanse. Rapporten nevner videre at rundt syv av ti, både blant annen maritim næring og i rederiene, gir uttrykk for at egen virksomhet mangler digital kompetanse i stor eller noen grad (Andersen, Bjørnset, & Rogstad, 2019).

Den ene dekksoffiseren er ingen motstander mot digitalisering på fartøy, men uttrykker at noen digitaliserte prosesser kan være vanskelig å forstå seg på i starten, før man ser logikken bak og da nytten det medfører. Ut ifra dette utsagnet kan det virke ut som at det finnes en interesse for å ta i bruk digitalisering på fartøy for den nytten det oppleves å medføre, selv om man begrunnet begrensninger i digital kompetanse kanskje vil oppleve at noen digitaliserte prosesser kan være kompliserte innledningsvis.

Videre kan det derfor tenkes at det ikke er en manglende interesse ved mannskapet på fartøy som setter begrensninger for digitalisering, men i stedet en noe innskrenket digital kompetanse. Det er endog ingenting i dette utsagnet som antyder at disse vanskene med å forstå noen digitaliserte prosesser har gått ut over sikker fartøydrift, ettersom kjerneverdien til mannskap

på fartøy omhandler sikker fartøydrift og dette utsagnet forteller om en opplevelse av digitalisering på fartøy som noe gunstig.

I rapporten fra Fafo blir det uttrykt en usikkerhet i den maritime næringen angående hva som eventuelt skal investeres i angående digitalisering. Videre beskrives dette som en type usikkerhet som fordrer strategisk ledelse i den enkelte virksomhet, der det i den sammenheng er relevant å betegne at ulike aktører vil ha ulik nytte av de tilgjengelige digitale løsningene (Andersen, Bjørnset, & Rogstad, 2019).

Den ene rederiansatte forteller om ulike informasjonsinteresser mellom sjøsiden og landsiden i et rederi, der sjøsiden har interesse for taktisk informasjon for taktiske valg og landsiden trenger strategisk informasjon for strategiske valg. At det tales for at det finnes ulike informasjonsinteresser mellom sjøsiden og landsiden kan vise til at digitalisering på fartøy har forskjellige funksjoner for sjøsiden og landsiden. Det kan derfor tenkes at det er ulike meninger mellom sjø- og landsiden angående hvilke digitale løsninger som burde satses på etter hvilke funksjoner som vil være mest hensiktsmessig.

Endog, kan det tenkes at det må foreligge et godt samarbeid mellom partene for at man skal kunne oppfylle informasjonsønskene for begge parter, da det kan argumenteres for at om man har interesse for taktisk informasjon, så kan det være avhengig av at man har strategisk informasjon og omvendt. Angående sikker fartøydrift er dette et mål for både sjøsiden og landsiden, men det kan tenkes at de ulike informasjonsinteressene mellom partene kan påvirke tilnærmingen deres til hva som skal til for å bedrive sikker fartøydrift.

Fafo-rapporten beskriver at krav til bemanning gjerne knyttes til sikkerhet og at det derfor er vesentlig i diskusjoner om digitalisering da dette omhandler antall sjøfolk om bord. I utgangspunktet er det Sjøfartsdirektoratet som bestemmer sikkerhetsbemanning, i henhold til forskrift om bemanning av norske skip, der sikkerhetsbemanning beskrives som den minste tillatte bemanning et fartøy kan ha ved operasjon (Andersen, Bjørnset, & Rogstad, 2019).

Den ansatte i det maritime teknologiselskapet forklarer at en del av engasjementet for digitalisering på fartøy omhandler at rederier utforsker hvordan man gjennom digitalisering kan bedrive sikker fartøydrift innenfor regelverket, med færre sjøfolk om bord.

Det blir ikke nevnt noe spesifikt angående hvordan engasjementet for digitalisering på fartøy kan tenkes å kunne muliggjøre sikker fartøydrift med færre sjøfolk om bord, og videre er fartøy veldig forskjellige i den forstand at alle har forskjellige operasjonsmønster. Videre, ettersom

det i forskriften om bemanning av norske skip forklares at sikkerhetsbemanning er den minste tillatte bemanning et fartøy kan ha ved operasjon, kan det tenkes at det ved digitalisering på fartøy endog blir krevende å kunne anslå et antall sjøfolk som må være om bord hvert enkelt fartøy for å kunne bedrive en sikker fartøydrift.

Dette kan videre antyde at eventuelle effekter som digitalisering medfører, kan være vanskelig å måle og at det derfor blir komplisert å tilpasse forholdet mellom digitalisering og antall sjøfolk på fartøyet på en god måte uten at dette går ut over sikkerhetsbemanning og dermed sikker fartøydrift. Videre, selv om det utforskes hvordan digitalisering kan tenkes å muliggjøre sikker fartøydrift med færre sjøfolk om bord, kan det tenkes at selv ved en større grad av digitalisering på fartøy, så vil man uansett etter hvert nå et punkt der digitaliseringen ikke klarer å erstatte visse nøkkelstillinger om bord knyttet til drift, og da må det eventuelt skje endringer i regelverket for at dette skal kunne være mulig. Det kan derfor tenkes at det på et punkt vil være lite hensiktsmessig å fortsette digitaliseringen på fartøy i et forsøk på å bedrive sikker fartøydrift med minst mulig menneskelige ressurser.

Fafo-rapporten forklarer at det er usikkerheter mellom maritime aktører angående hvilken teknologi man skal investere i angående digitalisering, der det uttrykkes at digitalisering medfører store kostnader og at det derfor er forskjeller mellom maritime aktører når det gjelder hvor stort handlingsrom de har for eventuelle feilinvesteringer (Andersen, Bjørnset, & Rogstad, 2019).

Den ansatte i det maritime teknologiselskapet tenker at digitalisering på fartøy er en sentral trend som vil tilta i styrke da rederier virker å oppleve reduserte kostnader ved fartøydriften som resultat av dette. Basert på dette utsagnet kan det virke ut som at det mest sentrale i vurderingen om hvorvidt man har interesse for å investere i teknologi for digitalisering på fartøy kanskje angår hvorvidt man tenker digitaliseringen vil gi avkastninger. Videre kan det tenkes at størrelsen på rederier vil avgjøre graden av investering i digitale løsninger man vil oppleve som hensiktsmessig da det kan virke ut som at det er nødvendig at man tørr å satse for at man skal kunne oppnå noen gevinster med digitalisering. Med dette tenkes det at en kanskje må være forberedt på at de positive effektene man venter på fra eventuell digitalisering først vil vises om man investerer over en viss grense avhengig av størrelsen på avdelingene på sjøsiden og landsiden i et rederi.

Videre, angående når dette eventuelt kan oppleves å ha positiv effekt på sikker fartøydrift samtidig som at kostnader kanskje reduseres, kan derfor tenkes å være avhengig av at man

finner en optimal balanse angående investering i digitalisering på fartøy og ønsket effekt basert på størrelsen på rederiet.

## 5.2 FORDELER MED DIGITALISERING

Det uttrykkes i Fafo-rapporten at digitalisering vil medføre mer fokus på system- og elektronikkompetanse, der kapteinen kanskje blir mer arbeidsleder da det viktige sjømannskapet blir overlatt til systemene, og at kapteinen dermed kanskje kan bruke mer tid på god ledelse og effektivisering av oppgaver ved fartøydriften (Andersen, Bjørnset, & Rogstad, 2019).

Den ene dekksoffiseren forteller at digitalisering på fartøy og automatisering av rutineoppgaver tillater et økt fokus på de oppgavene man anser som viktigst, der man kan bruke frivakter mer hensiktsmessig, og at digitalisering derfor hjulpet med å bedrive en sikker fartøydrift. Dette utsagnet kan antyde at digitalisering på fartøy bidrar med at det blir et tydeligere skille mellom arbeidstid og fritid i et fartøysamfunn, der det sentrale i dette utsagnet er at digitalisering på fartøy og automatisering av rutineoppgaver gjør at frivaktene kan brukes mer hensiktsmessig. Dette taler for at man kanskje får bedre kvalitet på hvilen mellom vakter, og at dette derfor videre resulterer i bedre kvalitet på vakter og en mer sikker fartøydrift.

At kvaliteten på hvilen mellom vakter blir bedre kan begrunnes med at det kan tenkes at automatiseringen av rutineoppgaver vil gjøre at det foreligger mindre rutineoppgaver man ikke strekker til å gjøre på gjeldende vakt, og at dette dermed vil medføre mindre stress frem til neste vakt. Der det kan tenkes at uten automatisering av rutineoppgaver, ville det foreligget flere rutineoppgaver man ikke strekker til å gjøre på gjeldende vakt, og at dette vil medføre mer stress. Dette i den forstand at man da vil tenke på dette til neste vakt og at frivakten derfor kanskje påvirkes negativt grunnet stresset dette kan medføre, og dermed reduserer kvaliteten på hvilen i tillegg til den påfølgende vakten.

Ut ifra dette utsagnet kan det også virke ut som at man gjennom digitalisering på fartøy ved automatisering av rutineoppgaver, også kan ha et større fokus på å utføre god ledelse. Videre kan dette tenkes å ha en positiv effekt på sikker fartøydrift, der det kan argumenteres for at en mangel på god ledelse kan føre til uønskede hendelser for sikker fartøydrift.

I Fafo-rapporten blir det beskrevet at man gjennom digitalisering og bedre utstyr for monitorering av fartøykomponenters helsestatus kan gå fra preventive til reaktive tiltak for vedlikehold av fartøykomponenter (Andersen, Bjørnset, & Rogstad, 2019).

Den ene dekksoffiseren uttrykker at digitalisering på fartøy og informasjonsinnsamling om fartøykomponenters faktiske helsestatus, tilrettelegger for et bedre grunnlag for å anslå vedlikeholdsintervaller på fartøykomponenter sammenlignet med tidsbaserte intervaller. Dette utsagnet kan antyde at digitalisering på fartøy har skapt en endring i den maritime næringen, der man har gått fra preventive tiltak knyttet til tidsbaserte vedlikeholdsintervaller, til reaktive tiltak knyttet til vedlikeholdsintervaller bestemt av fartøykomponenters faktiske helsestatus.

Dette kan i første rekke tenkes å medføre klare økonomiske gevinster for den maritime næringen. Hvorvidt denne endringen kan tenkes å ha en positiv effekt på sikker fartøydrift kan dermed diskuteres. I tilfeller der vitale fartøykomponenter som fremdriftsmaskineri eventuelt skulle få problemer tidligere enn antatt, og kanskje slutte å fungere. Der det videre kan antyde at den tidsbaserte vedlikeholdsplanen ikke har stemt overens med de faktiske belastningene fartøykomponenten har blitt påført, så vil dette kunne tenkes å utgjøre en fare for sikker fartøydrift. Videre kan dette begrunnes med at man uten fungerende fremdriftsmaskineri ikke kan kontrollere fartøyets bevegelse gjennom vannet.

Det kan derfor tyde på at man gjennom informasjonsinnsamling på fartøykomponenter om faktisk helsestatus vil være hensiktsmessig for sikker fartøydrift. På den andre siden, da det allerede foregår rutinemessig kontroller av vitale fartøykomponenter for å forebygge eventuelle problemer, så kan dette tale for at det bare er økonomiske gevinster med dette. Videre kan man argumentere for at det kan være feil ved sensorer og at man dermed uansett ikke kan tillate å blindt stole på den angitte helsestatusen til fartøykomponentene.

I rapporten fra Fafo blir det uttrykt at sjøfolkene trolig etter hvert vil havne i en helt ny arbeidssituasjon som følger av digitalisering og digitale løsninger som fjerntilgang til fartøy fra land, og at dette fordrer at sjøfolkene innehar en viss digital kompetanse. Rapporten fra Fafo fant også at 97 prosent er helt eller delvis enige i at fremtidens sjøfolk må inneha både digital kompetanse så vel som den maritime for å oppdatere, vedlikeholde og reparere de digitale løsningene på fartøy (Andersen, Bjørnset, & Rogstad, 2019).

Den ene dekksoffiseren, den ene rederiansatte og den ansatte i det maritime teknologiselskapet uttrykker at digitalisering på fartøy og fjerntilgang til fartøy fra land har bidratt med å knytte fartøy og rederikontor nærmere hverandre og gjort det lettere å motta hjelp til å utbedre feil ved digitale løsninger på fartøyet. Basert på dette kan det virke ut som at digitalisering og fjerntilgang til fartøy fra land har ført fartøy og rederikontor nærmere enn de kanskje var før og at det kanskje har kommet bedre metoder for å utbedre problemer gjennom fjerntilgang. Da

det uttales at digitalisering på fartøy har bidratt med å knytte fartøy og rederikontor nærmere, kan det tenkes at det har foreligget et ønske mellom de om å oppnå en bedre forståelse av sjø- og landsiden i et rederi sin forskjellige hverdag for å kunne samarbeide bedre.

Det kan videre virke som at man nå for tiden kanskje klarer å utføre oppdateringer, vedlikehold og reparasjon av flere fartøykomponenter enn det som tidligere var mulig, og at dette har redusert behovet for at mannskap på fartøy skal inneha digital kompetanse til å kunne bedrive denne aktiviteten.

Det kan også tenkes at det er ønskelig fra både sjøsiden og landsiden i et rederi om å fortrinnsvis søke hjelp fra fagekspertise, siden det kan tenkes at den begrensede digitale kompetansen både på fartøy og rederikontor kan være et hinder for å kunne håndtere slike problem. Hvorvidt det at man kanskje trenger fagekspertise, som ofte ikke er innad i rederiet og man må søke ekstern hjelp, kan være et problem for sikker fartøydrift er vanskelig å fastslå. Det kan tenkes at når man må belage seg på eksterne aktører så vil det ta en lengre stund å fikse problemer enn om man kunne ordnet problemene selv, der denne stunden videre kan tenkes å påvirke sikker fartøydrift negativt om problemene angår digitale løsninger for å beholde kontrollen på fartøyet. Endog kan det argumenteres for at siden det finnes måter for å beholde kontrollen over et fartøy, uavhengig av eventuelle problemer ved digitale løsninger, så vil ikke feil ved digitale løsninger som ikke blir utbedret hurtig nok uansett gå ut over sikker fartøydrift.

Fafo-rapporten beskriver at digitalisering og riktig analysering av store mengder innsamlede data fra fartøy vil kunne øke effektiviteten ved fartøydriften (Andersen, Bjørnset, & Rogstad, 2019). De rederiansatte og den ansatte i det maritime teknologiselskapet forteller at digitalisering på fartøy og informasjonsinnsamling muliggjør sammenstilling av informasjon fra flere og nøyaktigere kilder slik at man kan utføre analyser på tvers for å skape en bedre oversikt over fartøyflåtens driftsprofiler og fremme sikker fartøydrift.

Ut ifra dette utsagnet kan det tenkes at det gjennom digitalisering på fartøy foreligger et ønske om å bruke stordataanalyser for å kunne bedre forstå fartøyflåtens driftsprofiler for å kanskje kunne tilpasse hva som anses som sikker fartøydrift for de forskjellige fartøyene i flåten. Det kan videre argumenteres for at man i bruken av stordataanalyser lettest vil merke påvirkningen angående økt effektivitet for fartøydriften.

Når det er nevnt, kan det tenkes at en positiv bivirkning til økt effektivitet for fartøydriften vil være at det kanskje åpner for at man kan utøve bedre ledelse på fartøyet og at det dermed fremmer sikker fartøydrift. På den andre siden er det et viktig poeng at effektiv fartøydrift ikke

alltid fører med seg sikker fartøydrift og omvendt. Dette begrunnes med at det kan tenkes at det finnes mange måter å effektivisere fartøydriften på, men der dette ville gått på bekostning av sikker fartøydrift og motsatt.

Det blir i spørreundersøkelsen fra Fafo-rapporten der det ble undersøkt hvordan den norske maritime næringen mente utviklingen innenfor digitalisering ville bidra med å styrke verdiskapingen i deres virksomhet, funnet ut at det er en stor tro på at digitalisering vil kunne styrke verdiskapingen for virksomhetene i maritim næring, der 63 prosent av rederiene og 73 prosent av de andre maritime virksomhetene mener at dette kan bidra i svært stor eller nokså stor grad (Andersen, Bjørnset, & Rogstad, 2019).

Alle de intervjuede i dette forskningsprosjektet uttrykker at digitalisering på fartøy, med hensyn til sikker fartøydrift og cybersikkerheten på fartøy, totalt sett oppleves som noe positivt. Basert på det at alle de intervjuede uttrykker dette, kan dette tale for at den maritime næringen i denne samtiden, som tilbake i 2019, fortsatt har troen på at digitalisering vil bidra med å styrke verdiskapningen.

Dette kan videre antyde at det i den maritime næringen fortsatt finnes grunnlag for å tenke at det foreligger flere fordeler å uthente i fra digitalisering angående sikker fartøydrift. Videre kan det virke som at når det gjelder cybersikkerhet på fartøy, så tenker den maritime næringen at eventuelle utfordringer for cybersikkerheten på fartøy og effekten eventuelle brudd på cybersikkerheten kan ha på sikker fartøydrift ikke vil være av noen betydelig grad.

På den ene siden kan det tenkes at utsagnet er preget av samtidens fokus på digitalisering i organisasjoner og at den maritime næringen derfor tenker de må være proaktive og bedrive digitalisering på fartøy for å kunne være konkurransedyktige. På den andre siden så kan det også tenkes at siden digitalisering virker å fremme sikker fartøydrift uten at det merkes å medføre særlige konsekvenser for cybersikkerheten på fartøy, så kan digitalisering på fartøy virke innlysende. Det kan kanskje tenkes her at man kan bli blind av alle gevinstene som digitalisering medfører i den forstand at man ikke klarer like lett å se at digitalisering kan medføre noen negative effekter for cybersikkerheten på fartøy.

Når dette er nevnt kan det tenkes at de intervjuede uttrykker dette på bakgrunn av størrelsen på organisasjonen de er en del av, der det kanskje er lettere å anse at digitalisering på fartøy totalt sett er positivt for sikker fartøydrift målt opp mot eventuelle utfordringer for cybersikkerheten på fartøy i større organisasjoner sammenlignet med mindre organisasjoner, da større organisasjoner har større handlingsrom enn mindre organisasjoner.

## 5.3 MÅLSETNINGER FOR SIKKER FARTØYDRIFT

(Borch, 2016) forklarer at man for å bedrive sikker fartøydrift samtidig som fartøydriften er effektiv, er det viktig å ha en god sikkerhetskultur på både sjøsiden og landsiden i et rederi. Det beskrives videre at sikkerhetskultur kan defineres som etablerte verdier, holdninger og handlingsmønstre blant de ansatte som fremmer oppmerksomhet og kontinuerlig søking etter tiltak som kan redusere risikoen for uønskede hendelser, der de ansatte opplever et felles ansvar for målsetninger, virkemidler og styringssystemer for å redusere risiko (Borch, 2016).

Dekksoffiserene og de rederiansatte uttrykker at de er opptatte av sikker fartøydrift og opplever at det på fartøy har blitt tilrettelagt for bruk av flere digitale løsninger på en hensiktsmessig måte for å oppnå målsetningen om sikker fartøydrift. Basert på dette virker det som at det foreligger en god sikkerhetskultur i rederiene da det uttrykkes fra både sjø- og landsiden i rederi at de er opptatte av sikker fartøydrift. Videre siden det oppleves at digitalisering på fartøy har vært hensiktsmessig for å oppnå målsetningen om sikker fartøydrift, kan dette tyde på at bruk av digitale løsninger har medført at det har blitt lettere å søke etter tiltak for å redusere risikoen for uønskede hendelser som truer sikker fartøydrift.

Videre kan det virke som at digitalisering på fartøy har bidratt med å vedlikeholde en god sikkerhetskultur, der hensiktsmessig bruk av digitale løsninger har gjort det enklere å effektivisere fartøydriften uten at dette har gått ut over sikker fartøydrift. Det blir ikke spesifisert noe videre om hva som har blitt endret mot det bedre for å oppnå målsetningen om sikker fartøydrift annet enn å tilrettelegge for bruk av flere digitale løsninger på fartøy, men det kan tenkes at enhver prosess som effektiviseres vil frigjøre kapasitet til å kunne bedrive en mer sikker fartøydrift.

Borch (2016) uttrykker at det å operere et fartøy innebærer risikoer med påfølgende konsekvenser for liv, helse, miljø og andre verdier, og at det derfor er viktig at ledelsen på fartøy og rederikontor yter god sikkerhetsledelse for å systematisk kunne eliminere risikoene for uønskede hendelser. Borch (2016) forklarer videre at sikkerhetsledelse kan defineres som beslutning, iverksetting, styring og kontroll med den hensikt å redusere disse risikoene knyttet til liv, helse, miljø og andre verdier, der dette fordrer isolering av risikofaktorer som ikke kan elimineres og definering av akseptabel risiko for fartøyet.

Dekksoffiserene og de rederiansatte opplever at det er et felles ansvar mellom sjø- og landsiden i et rederi om å fremme gode bidrag for å oppnå målsetningen om sikker fartøydrift. Dette utsagnet kan antyde at det er en god forståelse fra ansatte på fartøy og rederikontor angående

at begge parter deler ansvaret om å oppnå målsetningen om sikker fartøydrift, der de på hver sin front må bidra med å fremme gode bidrag med hensyn til god sikkerhetsledelse. Dette kan videre antyde at det oppleves å være et balansert ansvarsforhold mellom sjø- og landsiden i rederi med hensyn til å bedrive god sikkerhetsledelse for å fremme sikker fartøydrift.

Hvorvidt ansvarsforholdet har endret seg som følger av digitalisering på fartøy er vanskelig å fastslå, men det kan tenkes at sjøsiden har et større ansvar for å utøve god sikkerhetsledelse for å oppnå målsetningen om sikker fartøydrift. Dette kan argumenteres for ved at det i første rekke er handlingene til mannskapet på fartøy som avgjør hvorvidt de utsetter seg for uønskede hendelser som vil påvirke sikker fartøydrift negativt. Videre kan dette argumenteres for med at det kan tenkes at selv om landsiden kan legge grunnlaget for en sikker fartøydrift gjennom å instruere alle ansatte i rederiet om hvordan man utøver god sikkerhetsledelse, så er sikker fartøydrift endog avhengig av at sjøsiden faktisk opererer med hensyn til dette grunnlaget.

Borch (2016) forklarer at ansvaret om at skipsbesetningen får tilstrekkelig oppfølging med hensyn til oppgaver de settes til å gjøre og ved implementering av ny teknologi, i henhold til regelverket, påhviler rederiet og skipsføreren.

Dekksoffiserene uttrykker at de opplever at rederienes størrelse betinger at digitalisering på fartøy og implementering av digitale løsninger gjennomføres på en god måte for å oppnå målsetningen om sikker fartøydrift og peker på tilfredsstillende oppfølging av sjøfolkene med relevant opplæring. Dette utsagnet kan tyde på at hvorvidt digitalisering på fartøy vil være hensiktsmessig for å oppnå målsetningen om sikker fartøydrift er bestemt av hvordan dynamikken i organisasjonen er, der det ofte kan bli vanskeligere å nå ut til alle enheter i større organisasjoner med tilfredsstillende oppfølging.

Videre, da det kan det tenkes at digitalisering på fartøy med hensyn til målsetningen om sikker fartøydrift, bare vil kunne oppnås om mannskapet har tilfredsstillende oppfølging. Kan dette tale for at man ikke kan undervurdere nødvendigheten av at mannskapet innehar den riktige kompetansen til å kunne bedrive sikker fartøydrift, når digitale løsninger benyttes for å løse oppgaver knyttet til fartøydriften.

Endog det beskrives at ansvaret for tilstrekkelig oppfølging påhviler rederiet og skipsføreren, kan dette utsagnet antyde at det er forskjellige oppfatninger angående om det er sjøsiden eller landsiden som har det største ansvaret for å utøve tilfredsstillende oppfølging angående digitalisering på fartøy og bruk av digitale løsninger. Det er kanskje nærliggende å tenke at oppfølgingen angående digitalisering burde hovedsakelig komme fra landsiden i rederiet, da

det også er landsiden i et rederi som tar beslutninger for digitalisering. Endog kan det argumenteres for at kanskje er komplisert å yte fullgod oppfølging fra landsiden i et rederi uten at sjøsiden selv må inneha en viss digital kompetanse på forhånd for at de to partene i et rederi skal kunne forstå hverandre.

Videre kan det tenkes at det kan være vanskelig å sikre at alle sjøfolk i et rederi erfarer at de har mottatt tilfredsstillende oppfølging med hensyn til digitalisering på fartøy og implementering av digitale løsninger, da det er store variasjoner mellom sjøfolk, så vel som rederiansatte, angående det digitale kompetansenivået de på forhånd innehar.

## 5.4 FORHOLD TIL CYBERSIKKERHET

ISM koden, støttet av IMO vedtak MSC.428(98), satte krav om at alle skipseiere og ledere skulle vurdere cyberrisikoen og implementere relevante tiltak i alle funksjoner i deres sikkerhetssystem, innen 1 januar 2021 (DNV). BIMCO (2020) forklarer at cybersikkerhet omhandler beskyttelse av IT og OT system, samt beskyttelse av informasjon og data, og at cybersikkerhet derfor er viktig på grunn av den mulige effekten eventuelle brudd ved cybersikkerheten kan ha på personell, fartøyet, miljøet, selskapet og last.

Samtlige av intervjupersonene indikerer at fokuset og bevisstheten rundt cybersikkerhet er økende, noe som kan tyde på at de forstår viktigheten av god cybersikkerhet. Både dekksoffiserene og de rederiansatte utrykker videre at de ikke har opplevd eller registrert noen cyberangrep mot fartøy eller rederikontor, og anser derfor cybersikkerheten i selskapet som god. Dette trenger dog ikke å bety at cybersikkerheten nødvendigvis er tilstrekkelig og feilfri, da det stadig finnes sikkerhetshull. Videre kan det derfor tenkes at selskapet kanskje ikke har blitt satt på de helt store prøvelsene angående å håndtere brudd på cybersikkerheten, og at det er derfor cybersikkerheten oppleves som god.

Den ansatte i det maritime teknologiselskapet mener at cybersikkerheten på fartøy er varierende, og at det kan begrunnes med at alle fartøy er ulike og derfor har ulike behov når det kommer til sikkerhetsutstyr og sikkerhetsstyring. Ut ifra dette kan det virke som at den ansatte i det maritime teknologiselskapet har en forståelse for hva som må gjøres for å dekke forskjellige fartøy sine behov for å bevare cybersikkerheten.

Borch (2016) beskriver at det er viktig å vite at selv om et rederi eller et annet selskap har høye ambisjoner og omfattende sikkerhetsstyringssystemer så kan uhellet skje, og at dette henger sammen med menneskelige faktorer angående hvordan mennesker observerer, handler og

påvirkes. Noen av disse faktorene er utdanning, erfaring og følelsen av ansvar og myndighet til individet.

Den ene dekksoffiseren nevner at god cybersikkerhet på fartøy er avhengig av hver enkelt person om bord sin adferd når de er koblet opp på fartøyets internett. Den andre dekksoffiseren nevner at han oppfatter at menneskelig svikt eller feilvurdering er årsaken til de fleste brudd på cybersikkerheten, og at det sjeldent skyldes svakheter ved de teknologiske sikkerhetsbarrierene på fartøy.

Med dette virker det som at dekksoffiserene har god forståelse angående cybersikkerhet og hvordan cyberangrep kan forekomme, og at forståelsen har økt når det gjelder viktigheten rundt cybersikkerhet for å avverge uønskede situasjoner i form av eventuelle cyberangrep. Videre kan dette tyde på at menneskene som bruker utstyret ombord trenger tilstrekkelig opplæring, da de mener det hovedsakelig er menneskelige feil som er grunnen til at man blir utsatt for cyberangrep. Det kan derfor tenkes at det kreves mer tilrettelagte praktiske øvelser som føles realistiske og virkelighetsnære, for å gi mannskapet om bord en bedre forståelse av hvor viktig cybersikkerhet er.

Den ansatte i det maritime teknologiselskapet uttrykker at han mener det er viktig at rederiene forstår hvordan de kan håndtere eventuelle risikoer for cybersikkerheten på fartøy som følger av digitalisering. Innenfor dette nevner de rederiansatte at de stadig mottar informasjon om endringer ved det globale trusselbildet for cybersikkerheten, der det derfor kan tenkes å være urealistisk med noen form for fullstendig cybersikkerhet på fartøy, da det samtidig ville medført tilnærmet null funksjonalitet ved digitaliseringen.

Dette kan antyde at det stadig endrende globale trusselbildet gjør det vanskelig for den maritime næringen å bedrive digitalisering på fartøy da det stadig må innføres nye sikringer for å hindre cyberangrep. Hvorvidt en generell god balanse mellom cybersikkerhet og funksjonalitet ved digitalisering endog hadde vært mulig å fremstille er vanskelig å bedømme. Når det er nevnt kan det tenkes at om man hadde lagt til grunn en generell god balanse mellom cybersikkerhet og funksjonalitet, så ville dette kanskje muliggjøre at man lettere kunne omstille seg og håndtere eventuelle uforutsette cyberangrep. Videre kan dette antyde at det bør være en form for sammenhengende samarbeid og kommunikasjon mellom rederier og fagkyndige innenfor cybersikkerhet for at man skal kunne balansere cybersikkerhet og funksjonalitet ved digitalisering på en god måte.

## 5.5 ULEMPER MED DIGITALISERING

Ifølge BIMCO kan det være ulike grunner til at et selskap blir utsatt for cyberangrep. Noen selskaper blir angrepet grunnet svakheter som er oppdaget av cyberangripere, mens andre bedrifter kan være spesifikke mål. Av de ulike typene cyberangripere tidligere nevnt, er det trolig cyberkriminelle som utgjør den største trusselen i maritim næring. Cyberkriminelle er som andre kriminelle, motivert av penger eller gods, og tar ofte i bruk utpressing for å oppnå målene sine (BIMCO, 2020).

Den ansatte i det maritime teknologiselskapet nevner i intervjuet at ulempen med digitalisering er at fartøy kan bli mer sårbare for cyberangrep. Dette i form av at digitalisering og bruk av omfattende dataanalyser, smarte fartøy og det industrielle tingenes internett vil øke mengden tilgjengelig informasjon for trusselaktører og den potensielle angrepsoverflaten for cyberkriminelle.

Cyberangrep er dog bare en, av flere ulemper med digitalisering. Både dekksoffiserer og rederiansatte nevner at digitaliseringen har ført til at enkelte sjøfolk føler seg overvåket, noe som kan tenkes å ha en negativ effekt på samspillet mellom sjø- og landsiden i et rederi. Det kan videre tenkes at dette kan medføre at enkelte blir motstandere av digitalisering og derfor kanskje ikke tar cybersikkerhet på alvor. Dette kan indikere at det finnes ulemper med digitalisering som ikke alltid er så lett å tenke over. Intervjupersonene viser god forståelse for dette, noe som kan være nyttig for å kunne komme opp med løsninger eller planer for å nøytralisere eller redusere ulempene.

Digitalisering har ført til at IT og OT systemer har kommet nærmere hverandre og er mer integrert. Forstyrrelser eller svikt i noen av disse systemene kan skape farlige situasjoner og føre til en betydelig risiko for sikkerheten om bord. Det poengteres derfor at investeringer knyttet til IT og OT systemer bør involvere noen som har forståelse for innvirkningen digitaliseringen kan ha på systemene om bord (BIMCO, 2020).

Det nevnes av den ene rederiansatte at det tenkes digitalisering på fartøy vil medføre at de i større grad blir avhengige av eksterne ressurser med fullverdig kompetanse innen cybersikkerhet for å bevare cybersikkerheten. Den rederiansatte uttrykker også at enkelte sjøfolk er skeptiske til at stadig flere fartøykomponenter skal være tilkoblet internett, da dette kan skape store problemer om fartøyet blir utsatt for cyberangrep. På bakgrunn av disse utsagnene kan dette antyde at det er forskjellige problemer ved integrering av IT og OT system på fartøy, der enkelte rederier virker usikre angående hvordan de kan opprettholde

cybersikkerheten uten å være avhengig av eksterne ressurser i form av fagkyndige innenfor cybersikkerhet.

Videre kan det tenkes at siden enkelte sjøfolk er skeptiske til at stadig flere fartøykompontenter skal være tilkoblet internett, så kan dette antyde en opplevelse av at nytteverdien er for lav med hensyn til et større potensial for farer som kan oppstå om man utsettes for cyberangrep og visse vitale fartøykomponenter blir misbrukt.

Den ene dekksoffiseren nevnte at digitaliseringen kan danne grunnlag for usunn konkurranse mellom like fartøy i et rederi, i form av intern konkurranse om å levere best mulig resultater for sitt fartøy, og at dette kan føre til at det blir tatt snarveier i form av unødvendige sjanser og risikoer.

Dette kan ha en sammenheng med at sjøfolk føler seg overvåket gjennom digitalisering på fartøy, og derfor føler press på å levere best mulig resultater. Dog det kan være bra for et rederi at søsterfartøy konkurrerer og pusher hverandre til å oppnå gode resultat, er det ikke bra om dette går på bekostning av sikkerhet og fornuft.

## 5.6 TILTAK FOR BEVARING AV CYBERSIKKERHET

Cyberrisikostyring bør være en innboene del av et selskaps trygghets- og sikkerhetskultur. Videre bør cyberrisikostyring bidra til trygg og effektiv operasjon av fartøyet og være implementert på ulike nivå i selskapet, inkludert personell om bord på fartøy og senior ledelsen på land (BIMCO, 2020).

Det kan argumenteres for at det er umulig for et rederi eller selskap å sikre seg helt mot cyberangrep, men at det finnes mange gode tiltak for å redusere risikoen for et mulig cyberangrep. Blant tiltakene som nevnt av BIMCO (2020) og (National Cyber Security Center) fant man blant annet oppdateringer, segregeringer, og gode passordrutiner.

Segregering innebærer at systemene ombord er koblet opp til ulike servere eller nettverk (BIMCO, 2020), noe som den ene dekksoffiseren viser at det er fokus på om bord i form av å bevisst skille mellom bruken av private datamaskiner tilkoblet fartøyets internett og datamaskiner direkte tilkoblet fartøyets digitale løsninger. Det kan tenkes at ved en sånn type segregering kan man beskytte seg mot cyberangrep, ved å hindre angripere tilgang på fartøysystemet.

Det kan tyde på at segregering er et fokusområde om bord på fartøy, og at det er et stort fokus på å skille mellom datamaskiner man bruker privat og datamaskiner som hører til fartøyet. De rederiansatte viser til tiltak de har for å bevare cybersikkerheten på fartøy ved at visse fartøykomponenter er frakoblet internett som standard, der fartøykomponentene bare tilkobles internett ved behov. Dette tiltaket har ifølge dem, gjort fartøy mindre sårbare for cyberangrep, da det ikke foreligger en kontinuerlig tilgang til fartøykomponentene ved at de ikke alltid er tilkoblet internett.

Oppdateringer og gode passordrutiner er andre viktige tiltak for bevaring av cybersikkerhet. Først og fremst er oppdateringer viktig for å unngå andre som utnytter programvarefeil, mens gode passordrutiner er viktig for å hindre angripere i å ha enkel adgang (BIMCO, 2020). Det er ingen av intervjupersonene som nevner oppdateringer og gode passordrutiner, men det trenger ikke nødvendigvis å bety at det er fraværende. Det er mye å holde styr på under ett intervju, og det kan nok tenkes at de har gode rutiner for oppdatering og passord, selv om intervjupersonene ikke nevnte dette.

Alle intervjupersonene viser gjennom intervjuene at de forstår viktigheten av cybersikkerhet, og at de er kjent med forskjellige tiltak som er nødvendige for å bevare cybersikkerheten på fartøy. Deriblant det at mannskapet skal være bevisste i sine handlinger tilkoblet fartøyets internett. Det nevnes også av enkelte intervjupersoner at mannskapet om bord stadig skal være varsomme og kritiske til e-poster som mottas fra mistenksomme sendere. Dersom slike mistenkelige e-poster er mottatt oppfordres det til å melde ifra om dette, slik at rederiet er opplyste om at lignende e-poster kan være i omløp.

Det fortelles videre av enkelte intervjupersoner at det aktivt gjøres en innsats for å forebygge mot cyberangrep, da det som regel er menneskelige feil som er årsaken, og at det derfor er nødvendig med opplæring av mannskap i cybersikkerhet. Den ene rederiansatte nevner at mannskapet utgjør den største cyberrisikoen, og at det derfor er viktig å øke bevisstheten rundt cyberangrep og bedre forståelsen av konsekvensene eventuelle angrep kan medføre.

Da det uttrykkes av den ansatte i det maritime teknologiselskapet at det er et felles ansvar mellom sjø- og landsiden for at cybersikkerhet blir tatt opp som en del av sikkerhetsrutinene på fartøy, kan dette antyde at det er et felles ansvar for alle i et rederi, både på fartøy og på land, at cybersikkerhet blir tatt på alvor og at gode rutiner og praksiser blir tatt i bruk.

## 5.7 PROSEDYRER OG RETNINGSLINJER

Borch (2016) forklarer at teknologien som blir benyttet for å drifte fartøy ofte er meget krevende. Videre uttrykker Borch (2016) at det derfor er viktig å bemerke at uhell fortsatt kan forekomme uavhengig av et rederi eller et annet selskaps høye ambisjoner og omfattende styringssystemer.

Den ene dekksoffiseren uttrykte at rederiet har utarbeidet prosedyrer angående cybersikkerhet på fartøy. Den andre dekksoffiseren fortalte derimot at rederiet ikke har utarbeidet prosedyrer, men i stedet en instruksjonsmanual angående cybersikkerheten på fartøy. Basert på disse utsagnene kan det virke som at det er forskjellige tilnærminger mellom rederi når det gjelder å innføre prosedyrer og retningslinjer for å bevare cybersikkerhet på fartøy, der det kan tenkes at rederier har forskjellige synspunkt angående cybersikkerhet, og da faremomentene som kan oppstå om man ikke har tilfredsstillende prosedyrer.

Det kan videre argumenteres for at siden digitalisering på fartøy medfører ytterligere krav til cybersikkerhet på fartøy, så kan det tenkes at prosedyrene må være utarbeidet på et godt grunnlag for at de skal være gunstige. Det er et kjent fenomen at uhell fortsatt kan forekomme selv om man tilrettelegger for at dette ikke skal skje. Det kan derfor tenkes at selv om prosedyrene er utarbeidet på et godt grunnlag, så vil eventuelle misforståelser eller dårlig etterlevelse av prosedyrer som følger av et begrenset kompetansegrunnlag for bevaring av cybersikkerhet, endog være en fare for cybersikkerheten på fartøy.

Det er i dag viktig at sikkerhetskulturen på fartøy også inkluderer cybersikkerhet. Selskapet PwC forklarer at sikkerhetskulturen er et virkningsfullt og naturlig virkemiddel for bevisstgjøring rundt informasjonssikkerhet, der sikkerhetskulturen kan bidra med å understreke viktigheten av at alle tar ansvar med å forsvare mot cyberangrep (PwC, 2022). Den ene dekksoffiseren og den ene rederiansatte uttrykte at det over en lengre periode har vært et fokus rettet mot cybersikkerhet på fartøy, men at fokuset angående dette økte etter at IMO-kravet om å innføre cybersikkerhet som en del av sikkerhetsstyringssystemet kom 1. januar 2021.

Det kan ut ifra disse utsagnene tenkes at cybersikkerhet lenge har vært en del av sikkerhetskulturen på fartøy, der innføringen av IMO-kravet hadde en videre effekt på å kanskje definere tydeligere hva som måtte gjøres for å bevare cybersikkerheten på fartøy og at dette derfor medførte et økt fokus angående cybersikkerhet på fartøy. Det kan argumenteres for at det vil være helt umulig for et rederi å gardere seg totalt mot cyberangrep uavhengig av en god sikkerhetskultur. Dette kan videre forklares ved at selv om det finnes gode løsninger og

tiltak for å minimere risikoen for å bli utsatt, så er cyberangrep sjeldent like i tillegg til at det stadig kommer nye måter å utføre cyberangrep på.

Dette kan derfor kanskje tale for at sikkerhetskultur bare hjelper et stykke på veien for å bevare cybersikkerhet på fartøy. Det kan også argumenteres for at IMO-kravet kanskje ikke er så veldig strengt i den forstand at det kan tolkes ganske vidt mellom rederier angående hvordan de vil innføre eventuelle prosedyrer og retningslinjer for å bevare cybersikkerheten. Det kan derfor tenkes at IMO-kravet kanskje burde være tydeligere for at det skal kunne tolkes som et strengere krav.

Samtidig kan dette motargumenteres med at siden cyberangrep som nevnt ofte forekommer på ulike måter og i tillegg på stadig nye måter, så vil det derfor kanskje være vanskelig å utarbeide tydeligere krav. Dette kan videre tale for at det kanskje burde være et mer kontinuerlig og tettere samarbeid mellom aktørene som fremstilte IMO-kravet og fagkyndige innenfor cybersikkerhet. Dette med den hensikt at et nærmere og mer kontinuerlig samarbeid kanskje ville kunne sammenstille IMO-krav med oppdaterte anbefalinger fra fagkyndige innenfor cybersikkerhet på en raskere måte. Videre kunne dette tenkes å derfor tilrettelegge for stadig oppdaterte IMO-krav, der disse kanskje også ville oppleves å være tydeligere slik at rederier kanskje har en klarere forståelse om hvordan de skal bevare cybersikkerheten på fartøy.

Det blir av Borch (2016) forklart at hvordan mennesker observerer og handler påvirkes av en rekke faktorer, der en av disse faktorene er utdanning. Den ene rederiansatte forteller at prosedyren deres for å bevare cybersikkerhet på fartøy hovedsakelig ble utarbeidet av rederiet selv, men forklarer at de underveis også gjennomgikk prosedyren med eksperter innen cybersikkerhet. Ut ifra dette kan det tenkes at problemene som løftes i forhold til cybersikkerhet på fartøy og utarbeiding av hensiktsmessige prosedyrer for cybersikkerhet er noe som er relativt nytt for rederier. Det virker derfor videre å være usikkerheter angående hvordan dette burde gjøres innenfor rederier, der det kanskje oppleves at man er nødt til å benytte seg av ekstern fagekspertise for at prosedyrene skal bli velfungerende.

Det kan virke som at rederier i oppfølgingen av digitalisering på fartøy med tilfredsstillende tiltak for cybersikkerheten, stadig blir mer avhengig av eksterne aktører for å sikre at prosedyrene er vanntette. Dette kan tenkes å være en faktor som kan bremse digitalisering på fartøy i den forstand at rederier må belage seg på eksterne aktører før de endrer prosedyrer. På samme tid kan dette tenkes å fremskynde at rederier tilegner seg nødvendig kompetanse innenfor cybersikkerhet, der om de ønsker å digitalisere på fartøy for å øke egen

konkurransedyktighet, må inneha kunnskap om cybersikkerhet for å kunne riktig tilpasse prosedyrer.

Mennesker observerer og handler på bakgrunn av en rekke faktorer der en faktor angår kommunikasjon mellom nivåene og avdelingene i organisasjonen (Borch, 2016). Den ansatte i det maritime teknologiselskapet tenker at uavhengig av innfallsvinkler for utarbeiding av prosedyrer for å opprettholde cybersikkerheten på fartøy, så er det viktigste at disse prosedyrene blir forstått riktig av sjøfolkene slik at prosedyrene kan virke etter tiltenkt hensikt.

Det kan tenkes at for å sikre at prosedyrer blir forstått riktig og dermed etterlevd på en riktig måte, så er man avhengig av god kommunikasjon mellom nivåene og avdelingene i en organisasjon. Et rederi kan forekomme i mange størrelser der det ofte er en sammenheng mellom størrelsen på rederier og hvor komplisert kommunikasjon mellom deler av rederiet kan være. Videre kan dette tale for at det ikke er gitt at sjøsiden forstår hvordan de skal etterleve prosedyrene på en tilfredsstillende måte, selv om prosedyrene innført av landsiden i et rederi blir distribuert til fartøy.

Siden det blir poengtert at det viktigste er at prosedyrene blir forstått slik at de får virket etter tiltenkt hensikt, kan dette antyde at det kanskje ikke er nødvendig for alle ansatte i et rederi å ha full oversikt over prosedyrene. Videre kan det derfor tenkes at det kanskje er nok at ansatte i nøkkelstillinger for cybersikkerheten på fartøy har en mer fullgod oversikt over prosedyrene. Dette kan argumenteres videre med at de ansatte i nøkkelstillingene kan fungere som en forsterkning av kommunikasjonen mellom delene av organisasjonen slik at man på denne måten sørger for å nå ut til alle ansatte og at alle ansatte dermed forstår prosedyrene til en god nok grad til å ikke utgjøre noen cyberrisiko.

## 5.8 OPPLÆRING OG ØVELSER

Borch (2016) uttrykker at opplæring må tilpasses hvert enkelt individ, der dette må kartlegges og planlegges. Det forklares videre at det mest gunstige innebærer samtaler med de ansatte for å anskaffe en klar oppfattelse av individets kunnskaper og erfaringer, slik at opplæringen kan gjennomføres på en mest hensiktsmessig måte (Borch, 2016).

Dekksoffiserene uttrykker at god opplæring er utslagsgivende for en sikker fartøydrift og forteller at de har fått opplæring knyttet til cybersikkerhet på fartøy. Den ansatte i det maritime teknologiselskapet forklarer videre at opplæringen bør ta hensyn til sjøfolkenes kompetansegrunnlag. Ut ifra at dette kan det tenkes at det kanskje finnes rom for å tilpasse

opplæringen der det blir tatt bedre hensyn til individene som opplæres sitt kompetansegrunnlag med hensyn til kunnskaper og erfaringer de eventuelt innehar på forhånd.

Det kan argumenteres for at det vil være store variasjoner i kompetansegrunnlaget mellom ansatte i et rederi. Videre om man da i gjennomføringen av opplæringen går ut ifra at de ansatte har et visst antatt kompetansegrunnlag, så kan dette tale for at de ansatte vil oppleve forskjellig utbytte av opplæringen. Dette kan videre forklares med at alle ansatte som har et større kompetansegrunnlag enn det antatte, vil ha et større utbytte av opplæringen og kanskje oppleve at de øker egen forståelse slik at de kan raffinere eget handlingsmønster. Når det kommer til de ansatte som har et mindre kompetansegrunnlag enn det antatte, kan det tenkes at de vil ha et mindre utbytte av opplæringen der de i tillegg kanskje ikke vil forstå hvordan de skal anvende det de har lært ved en senere anledning.

Videre kan det tenkes at selv om rederiene har iverksatt øvelser og opplæring omkring temaet cybersikkerhet som følger av IMO-kravet, har det kanskje ikke blitt fremført krav som er tydelige nok. Det kan videre argumenteres for at om kravene ikke er tydelig nok vil det bli opp til rederier å vurdere hva som tilsier god opplæring. Dette kan videre være uheldig for opplæringens karakter, da rederier ofte ikke innehar et tilstrekkelig kompetansegrunnlag for å vurdere dette basert på deres faglige bakgrunn.

BIMCO uttrykker at cyberrisikostyring bør inneholde identifisering av roller og ansvar til ansatte i et rederi, identifisering av systemets særegenhet og sårbarheter, implementering av tekniske og prosedyremessige anordninger og en beredskapsplan (BIMCO, 2020).

Den ene dekksoffiseren gir uttrykk for at rederiet har utsendt e-læringskurs angående opplæring i cybersikkerhet på fartøy, men at disse oppleves å bli for overfladiske og at det derfor ønskes mer håndfast opplæring der det pekes på uanmeldte saksbaserte øvelser angående cybersikkerhet på fartøy. Dette utsagnet kan antyde at det er en forståelse for nødvendigheten av å utøve god cyberrisikostyring for å bevare cybersikkerheten på fartøy. Det kan tenkes at e-læringskurs bare vil fungere som en innledningsvis opplæring i hva som forventes for å utøve cyberrisikostyring. Videre kan det derfor argumenteres, på bakgrunn av at det uttrykkes et ønske om mer håndfast opplæring, at en ikke klarer å oppnå et tilfredsstillende kompetansegrunnlag gjennom e-læringskurs.

Det som ville vært et tilfredsstillende kompetansegrunnlag kan tenkes å naturlig måtte ta utgangspunkt i hva cyberrisikostyring bør inneholde. Det kan derfor tenkes at kompetanse om å identifisere roller og ansvar, identifisere sårbarheter for systemer og implementeringer av

tekniske og prosedyremessige tiltak og en beredskapsplan vil være essensielt for at opplæringen skal ha en hensikt. Det kan derfor tenkes at uanmeldte saksbaserte øvelser i form av forskjellige scenarioer for cyberangrep mot fartøy kunne hjulpet med å avdekke eventuelle kompetansemangler samtidig som å forsterke kompetansegrunnlaget for sjøfolkene om cybersikkerhet på fartøy.

Dette kan videre utdypes ved at man kanskje hadde fått kontrollert hvorvidt sjøfolkene inntok roller og tok ansvar. Videre kan det tenkes at man hadde fått testet hvorvidt sjøfolkene klarer å identifisere hvilke systemsårbarheter som kan ha blitt utnyttet i cyberangrepet. Samtidig kan det tenkes at slike uanmeldte saksbaserte øvelser kan bidra med å bedømme hvor gode de tekniske og prosedyremessige tiltakene og beredskapsplanen fungerer i sammenheng med menneskelige handlingsmønster om man blir utsatt for et cyberangrep mot fartøy.

BIMCO forklarer at det er viktig å forhøre seg med fagkyndige innenfor cybersikkerhet for å vurdere cyberrisikoer som følge av implementering av OT-systemer, der de uttrykker at forstyrrelser av OT-system kan medføre en betydelig sikkerhetsrisiko for mannskap, last, skade på det marine miljøet og hindring av fartøydriften (BIMCO, 2020). Intervjupersonen i fra det maritime teknologiselskapet forteller at opplæring innenfor cybersikkerhet på fartøy bør gjenspeile det gjeldende behovet for cybersikkerhet som følge av den gjeldende digitaliseringen på fartøy for at sjøfolk skal være best rustet til å håndtere cyberangrep.

Det kan tenkes at om det gjeldende behovet for cybersikkerhet på fartøy som følger av den gjeldende digitaliseringen ikke er balansert, vil dette kunne utgjøre en sikkerhetsrisiko for mannskap, last, skade på det marine miljøet og hindring av fartøydriften. Videre kan dette argumenteres for ved at om cybersikkerheten skal opprettholdes, så er man avhengig av at mannskapet også har opplæring som reflekterer fartøyets faktiske behov for cybersikkerhet slik at digitaliseringen kan foregå kontrollert. Det kan tales for at om det hadde vært ubalanse mellom det gjeldende behovet for cybersikkerhet og den gjeldende digitaliseringen, så kan dette tenkes å medføre at man er mer sårbar for cyberangrep mot fartøy i tillegg til at mannskapet kanskje ikke har holdbar opplæring for å hanskes med cyberangrepene på en god måte.

Videre vil denne ubalansen mellom cybersikkerhet og digitalisering, der cybersikkerheten nedprioriteres uten at man kanskje skjønner konsekvensene av dette og hvilke uheldige situasjoner man kan komme opp i, kanskje kunne tilskrives forskjellig modenhet angående cybersikkerhet mellom rederier. Dette kan videre uttrykkes ved at kanskje umodne rederier i

forhold til modne rederier angående cybersikkerhet på fartøy vil lettere kunne trå feil når det gjelder å tilrettelegge med tilfredsstillende opplæring i cybersikkerhet, der de kanskje mangler kompetansegrunnlaget for å bedømme hvilke momenter som burde være med i opplæring for å bevare cybersikkerheten.

## 5.9 OPPSUMMERING

I dette delkapittelet vil de foregående drøftede subkategoriene bli oppsummert der hovedpunktene vil bli trukket frem.

Det foreligger i denne samtiden et tydelig engasjement for digitalisering på fartøy i den maritime næringen, da det oppleves at man gjennom å implementere digitale løsninger, klarer å forenkle og forbedre mange prosesser knyttet til sikker fartøydrift både fra sjø- og landsiden av et rederi. Videre virker engasjementet for digitalisering å være tiltakende, der dette kan tilskrives at den maritime næringen stadig tenker at det eksisterer flere fordeler knyttet til sikker fartøydrift som enda ikke er uthentet, der disse tenkes å kunne realiseres gjennom digitalisering.

Det forklares videre av alle intervjuede at digitalisering på fartøy virker å medføre flere fordeler enn ulemper for den maritime næringen, med hensyn til henholdsvis gevinster gjennom digitalisering og utfordringer ved cybersikkerheten. Dette viser at den maritime næringen opplever at digitalisering totalt sett vil bidra med å styrke verdiskapningen i den maritime næringen.

Det oppleves at cybersikkerheten på fartøy er god i denne samtiden. Endog poengteres det at hvorvidt cybersikkerheten opprettholdes er avhengig av mannskapets handlinger, da det forklares at menneskelig svikt oftest er årsaken til at fartøy utsettes for cyberangrep. Videre blir det beskrevet et behov for mer tilfredsstillende opplæring angående cybersikkerhet, der det uttrykkes at saksbaserte øvelser hadde vært hensiktsmessig for å bedre utbyttet av opplæringen.

Det er videre en god forståelse av at digitalisering på fartøy gjør fartøyet mer sårbart for cyberangrep, der det nevnes at det innført en rekke tiltak med hensikt til å forebygge brudd på cybersikkerheten. Når det gjelder disse tiltakene, så anses det viktigste tiltaket å omhandle det å bevisstgjøre mannskap i sine handlinger gjennom god opplæring.

Det uttrykte kompetansegrunnlaget som beskrives i den maritime næringen angående bevaring av cybersikkerhet er varierende, der det virker som at opplæringen ikke er hensiktsmessig. Videre kan dette tale for at det kanskje finnes rom for å tilpasse opplæringen slik at den tar bedre hensyn til forskjeller i forhåndskunnskaper mellom mannskap på fartøy. Videre vil

kompetansegrunnlaget knyttet til å bevare cybersikkerhet på fartøy være sentralt for å kunne balansere den gjeldende digitaliseringen på fartøy med det påfølgende behovet for cybersikkerhet for at digitaliseringen skal foregå kontrollert.

Det beskrives videre at å balansere digitalisering og cybersikkerhet på fartøy fordrer at mannskapet har opplæring innen cybersikkerhet som reflekterer fartøyets aktuelle behov for cybersikkerhet som følge av digitaliseringen slik at fartøyet ikke er eksponert for uante faremomenter knyttet til cyberangrep som kanskje ikke mannskapet har holdbar nok opplæring til å hanskes med på en tilfredsstillende måte.

# 6.0 AVSLUTNING

Hensikten med denne studien har vært å innhente betraktninger angående de opplevde påvirkningene digitalisering har hatt for sikker drift og cybersikkerhet på fartøy, i tillegg til å finne ut hvorvidt digitaliseringen sitt helhetlige bidrag oppleves å gi flest fordeler eller ulemper for den maritime næringen.

Denne studien har gitt et innblikk i drivkrefter ved digitalisering knyttet til sikker fartøydrift, hvilke utfordringer digitalisering frembringer knyttet til cybersikkerhet og hvordan kompetansegrunnlaget knyttet til bevaring av cybersikkerhet er i den maritime næringen.

Funnene i denne studien viser at det foreligger et tydelig engasjement for digitalisering i den maritime næringen som trolig vil vedvare da digitalisering har medført en rekke fordeler og vært formålstjenlig for å oppnå målsetninger om sikker fartøydrift. Funnene viser også at digitaliseringen sitt helhetlige bidrag oppleves å gi flere fordeler enn ulemper for den maritime næringen. Funnene viser videre at den maritime næringen er bevisste på hvilke utfordringer digitalisering fører med seg knyttet til cybersikkerhet, men at det virker som at kompetansegrunnlaget for bevaring av cybersikkerhet ikke alltid samsvarer med ambisjonene innenfor digitalisering.

Det ser ut som at kompetansegrunnlaget for bevaring av cybersikkerhet ikke alltid samsvarer med ønskene om digitalisering på fartøy på grunn av lite hensiktsmessig opplæring innen cybersikkerhet. Forskningsgruppen har derfor valgt å utarbeide noen anbefalinger basert på relevante momenter tatt opp i denne studien:

- Rederiene burde i samarbeid med mannskapet på fartøy og fagkyndige innenfor cybersikkerhet utarbeide relevante og realistiske saksbaserte øvelser knyttet til cybersikkerhet og cyberangrep mot fartøy.
- Rederiene burde i samarbeid med mannskapet på fartøy tilrettelegge for at alle ansatte innehar tilstrekkelig opplæring innen cybersikkerhet ved å tilpasse opplæringen til de ansattes kunnskapsnivå.
- Cybersikkerhet burde innføres som en del av utdanningen til ansatte i lederstillinger på fartøy og rederikontor.

# REFERANSER


Andersen, R., Bjørnset, M., & Rogstad, J. (2019). *Maritim kompetanse i en digital framtid.* Oslo: Fafo.

Aubert, V. (1985). *Sosiologi.*

Aven, T. (2019, september 26). Hentet fra https://snl.no/risiko

BIMCO. (2020). *The Guidelines on Cyber Security Onboard Ships Version 4.* Hentet fra The Guidelines on Cyber Security Onboard Ships.

BIMCO. (2022, mai 10). *www.bimco.org*. Hentet fra Maritime digitalisation: https://www.bimco.org/Ships-ports-and-voyage-planning/Maritime-digitalisation

Borch, O. J. (2016). *Fartøyledelse og kontroll av skipets drift.* Bergen: Fagbokforlaget.

Dalland, O. (2012). *Metode og oppgaveskriving.* Oslo: Gyldendal Norsk Forlag.

Dalland, O. (2020). *Metode og oppgaveskriving.* Oslo: Gyldendal Norsk Forlag.

Digital21. (2018). *Digitale grep for norsk verdiskaping.* Oslo: Digital21.

DNV. (u.d.). *www.dnv.com*. Hentet fra Maritime cyber security: https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/ism-guidance.html

Dvergsdal, H. (2021, desember 1). *www.snl.no*. Hentet fra Digitalisering: https://snl.no/digitalisering

Heine Nätt, T. (2022, februar 16). *www.snl.no*. Hentet fra Cybersikkerhet: https://snl.no/cybersikkerhet

Heine Nätt, T. (2022, mars 21). *www.snl.no*. Hentet fra Hacking: https://snl.no/hacking

Heine Nätt, T., & Heide, C. (2021). *Datasikkerhet: ikke bli svindlerens neste offer.* Gyldendal.

IMO. (2017, juni 16). *wwwcdn.imo.org.* Hentet fra IMO: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

Inmarsat. (2020). *www.inmarsat.com.* Hentet fra Insights: https://www.inmarsat.com/en/insights/maritime/2020/digitalisation-uncovered.html

Itarian. (2022, mai 31). Hentet fra https://www.itarian.com/patch-management.php

Kvale, S., & Brinkmann, S. (2015). *Det kvalitative forskningsintervju.* Oslo: Gyldendal akademisk.

Malterud, K. (2017). *Kvalitative forskningsmetoder for medisin og helsefag.* Oslo: Universitetsforlaget.

National Cyber Security Center. (u.d.). *www.ncsc.gov.uk*. Hentet fra Passwords, passwords everywhere: https://www.ncsc.gov.uk/blog-post/passwords-passwords-everywhere

NHO. (2017). *www.arbinn.nho.no*. Hentet fra Sikkerhetskultur: https://arbinn.nho.no/hms/sikkerhet-og-beredskap/sikkerhet/sikkerhet/sikkehetskultur/

Nilstun, C. (2021, november 8). *www.snl.no*. Hentet fra Proxy: https://snl.no/proxy

Norges Rederiforbund. (u.d.). *www.rederi.no*. Hentet fra Digitalisering: https://rederi.no/om-oss/fagomrader/naringspolitikk/arctic-business/

NSM. (u.d.). *Nasjonal Sikkerhets Myndighet*. Hentet fra https://nsm.no/aktuelt/passordanbefalinger-fra-nasjonal-sikkerhetsmyndighet

Nærings- og fiskeridepartementet. (2020). *Grønnere og smartere - morgendagens maritime næring.*

PwC. (2022, mai 31). *www.pwc.no*. Hentet fra Hva er cybersikkerhet?: https://www.pwc.no/no/teknologi-omstilling/hva-er-cybersikkerhet.html

Store norske leksikon. (2020, november 4). *www.snl.no*. Hentet fra BIMCO: https://snl.no/BIMCO

Store norske leksikon. (2020, desember 29). *www.snl.no*. Hentet fra Dynamisk Posisjonering: https://snl.no/dynamisk_posisjonering

Wikipedia. (2022, mai 19). *no.wikipedia.org*. Hentet fra ISM-koden: https://no.wikipedia.org/wiki/ISM-koden

# VEDLEGG 1: GODKJENNING AV FORSKNINGSPROSJEKTET FRA NSD



NSD NORSK SENTER FOR FORSKNINGSDATA

# Vurdering

**Referansenummer**

808925

**Prosjekttittel**

Digitalisering knyttet til effektiv drift og cybersikkerhet på fartøy

**Behandlingsansvarlig institusjon**

Norges teknisk-naturvitenskapelige universitet / Fakultet for ingeniørvitenskap / Institutt for havromsoperasjoner og byggteknikk

**Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)**

Marie Haugli Larsen, marie.h.larsen@ntnu.no, tlf: 45061300

**Type prosjekt**

Studentprosjekt, bachelorstudium

**Kontaktinformasjon, student**

Andreas Mulelid Kvam, ammkvam@stud.ntnu.no, tlf: 41562544

**Prosjektperiode**

01.01.2022 - 30.06.2022

**Vurdering (1)**

---

**10.02.2022 - Vurdert**

Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar med personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet med vedlegg, og eventuelt i meldingsdialogen mellom innmelder og Personverntjenester. Behandlingen kan starte.

TYPE OPPLYSNINGER OG VARIGHET
Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til den datoen som er oppgitt i meldeskjemaet.

LOVLIG GRUNNLAG
Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake.

Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

PERSONVERNPRINSIPPER
-Personverntjenester vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen om:
-lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen
-formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke behandles til nye, uforenlige formål
-dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet
-lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet

DE REGISTRERTES RETTIGHETER
Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), og dataportabilitet (art. 20).

Personverntjenester vurderer at informasjonen om behandlingen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13.

Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

FØLG DIN INSTITUSJONS RETNINGSLINJER
Personverntjenester legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32).

Ved bruk av databehandler (spørreskjemaleverandør, skylagring eller videosamtale) må behandlingen oppfylle kravene til bruk av databehandler, jf. art 28 og 29. Bruk leverandører som din institusjon har avtale med.

For å forsikre dere om at kravene oppfylles, må dere følge interne retningslinjer og/eller rådføre dere med behandlingsansvarlig institusjon.

MELD VESENTLIGE ENDRINGER
Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til oss ved å oppdatere meldeskjemaet. Før du melder inn en endring, oppfordrer vi deg til å lese om hvilke type endringer det er nødvendig å melde: https://www.nsd.no/personverntjenester/fylle-ut-meldeskjema-for-personopplysninger/melde-endringer-i-meldeskjema

Du må vente på svar fra oss før endringen gjennomføres.

OPPFØLGING AV PROSJEKTET
Personverntjenester vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til med prosjektet!

# VEDLEGG 2: INFORMASJONSSKRIV OG SAMTYKKEERKLÆRING

## Vil du delta i forskningsprosjektet

### *"Digitalisering knyttet til effektiv drift og cybersikkerhet på fartøy"?*

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å finne ut om hvordan den maritime næringen både på sjø og land opplever at økt bruk av digitalisering i form av fjerntilgang fra land påvirker driften og cybersikkerheten om bord på fartøy. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva en eventuell deltakelse vil innebære for deg.

**Formål**
Formålet med dette forskningsprosjektet er å undersøke forholdet aktører i den maritime næringen har til digitalisering i form av fjerntilgang til fartøy fra land, med hovedfokus på å studere hvorvidt teknologien fremmer effektivitet eller skaper utfordringer knyttet til effektiv drift og cybersikkerhet på fartøy.
Dette prosjektet er en bacheloroppgave skrevet ved NTNU i Ålesund.

**Hvem er ansvarlig for forskningsprosjektet?**
NTNU er ansvarlig for prosjektet.

**Hvorfor får du spørsmål om å delta?**
Det ønskes å innhente relevant informasjon til forskningsprosjektet og anser derfor deg som aktør i den maritime næringen som en adekvat kilde.

**Hva innebærer det for deg å delta?**
En eventuell deltakelse i forskningsprosjektet innebærer for deg det å være med på et digitalt eller fysisk intervju, der opptak blir gjennomført for senere transkripsjon og analyse for å brukes i forskningsprosjektet. Opptaket blir slettet etter sensurfrist av forskningsoppgaven vår i utgangen av juni 2022. Intervjuet vil vare fra rundt 30 minutter og opptil 60 minutter.

**Det er frivillig å delta**
Det er frivillig å delta i forskningsprosjektet. Hvis du velger å delta, kan du når som helst trekke tilbake samtykket 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.

- De som vil ha tilgang til informasjonen som blir innhentet er vi tre studentene som skriver forskningsprosjektet; Magnus Gjerde, Andreas Sørum og Andreas Kvam, samt veileder; Marie Haugli Larsen.
- Personopplysningene dine vil bli erstattet med en kode som lagres på en egen navneliste adskilt fra øvrige data.

Deltakere i forskningsprosjektet vil bli anonymiserte, om ikke annet er ønskelig.

**Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?**
Datamaterialet skal slettes ved avslutning av forskningsprosjektet som etter planen er etter sensurfrist i utgangen av juni 2022.

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

På oppdrag fra NTNU har NSD – Norsk senter for forskningsdata AS 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:

- Veileder: Marie Haugli Larsen ved NTNU
  - Epost: marie.h.larsen@ntnu.no
  - Telefonnummer: 450 61 300

- Vårt personvernombud: Thomas Helgesen ved NTNU
  - Epost: thomas.helgesen@ntnu.no
  - Telefonnummer: 930 79 038

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

- NSD – Norsk senter for forskningsdata AS på epost (personverntjenester@nsd.no) eller på telefon: 53 21 15 00.

Med vennlig hilsen

| | |
|---|---|
| Marie Haugli Larsen | Magnus Gjerde |
| Veileder | Student |

---

# Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *Digitalisering knyttet til effektiv drift og cybersikkerhet på fartøy*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ å delta i intervju

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet, omtrentlig i utgangen av juni 2022.

---

(Signert av prosjektdeltaker, dato)

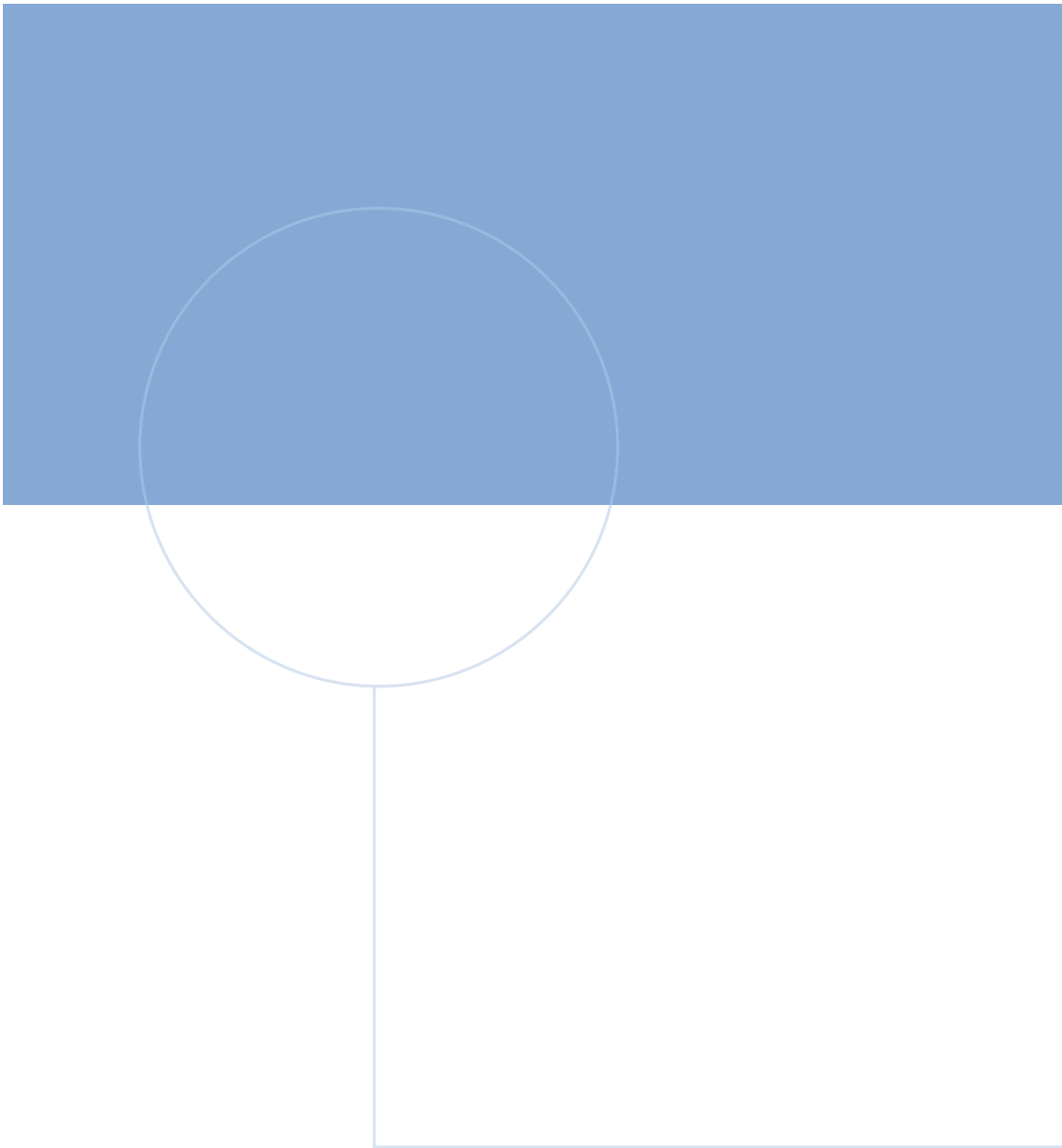
## VEDLEGG 3: INTERVJUGUIDER

| Intervjuguide 1 | Dekksoffiserer på fartøy og kontoransatte i rederi |
|---|---|
| **Hva vi ønsker å vite noe om** | **Forslag til spørsmål** |
| 1. Informasjon før intervjuet starter | Si litt om temaet for samtalen (bakgrunn, formål)<br><br>Forklar hva intervjuet skal brukes til, og forklar taushetsplikt og anonymitet<br><br>Spør om noe er uklart og om intervjupersonen har noen spørsmål<br><br>Informer og få samtykke til å starte opptak av intervju |
| 2. Personalia | Utdanning<br><br>Års erfaring<br><br>Nåværende stilling |
| 3. Grunnlag | Hva er deres forhold til digitalisering?<br><br>Hva er deres forhold til effektiv drift av fartøy?<br><br>Hva er deres forhold til forsvarlig cybersikkerhet? |
| 4. Bidrag | Hvordan arbeider dere med digitalisering i organisasjonen?<br><br>Hvordan arbeider dere med å fremme effektiv drift av fartøy i et organisasjonsperspektiv?<br><br>Hvordan arbeider dere med å bevare en forsvarlig cybersikkerhet i et organisasjonsperspektiv? |
| 5. Effektiv drift av fartøy<br><br>5.1. Generelt om effektiv drift av fartøy | Hvordan arbeider dere generelt for å fremme effektiv drift av fartøy?<br><br>Vil dere si at ansvaret om å fremme effektiv drift av fartøy ligger på sjøsiden eller landsiden? |
| Effektiv drift av fartøy<br><br>5.2. Digitalisering i form av datainnsamling på fartøy | Hva er deres forhold til digitalisering i form av datainnsamling på fartøy?<br><br>Om bedriften har et forhold til denne typen digitalisering: Er det datainnsamlingsteknologi fra Kongsberg Digital med Vessel Insight, Maress eller andre som brukes?<br><br>Om bedriften har et forhold til denne typen digitalisering: Til hvilken grad har bedriften deres tatt i bruk teknologi som muliggjør datainnsamling på fartøy? |

| | |
|---|---|
| | Om bedriften har et forhold til denne typen digitalisering: Har dette fremmet effektiv drift og forsvarlig cybersikkerhet på fartøy?<br><br>Om bedriften har et forhold til denne typen digitalisering: Hvordan opplever dere at denne allerede implementerte teknologien påvirker dere?<br><br>Om bedriften ikke har et forhold til denne typen digitalisering: Ser dere for dere at datainnsamlingsteknologi ville fremmet effektiv drift og cybersikkerhet på fartøy?<br><br>Om bedriften ikke har et forhold til denne typen digitalisering: Hvordan opplever dere at en eventuell implementering av denne typen digitalisering ville påvirket dere? |
| 6. Forsvarlig cybersikkerhet,<br><br>6.1. Oversikt over cybertrusler | Hvordan opplever du cybersikkerheten på fartøy per. 2022?<br><br>Har dere en oversikt over hvilke cyberangrep som er mest utbredt på fartøy?<br><br>Om cybersikkerheten oppleves bra: Hva tror du er grunnen til det? Har det med rutiner, prosedyrer, øvelser, bevisstgjørende arbeid osv. å gjøre?<br><br>Om cybersikkerheten oppleves dårlig: Hva tror du er grunnen til det, og hva burde gjøres? |
| Forsvarlig cybersikkerhet<br><br>6.2. Motstandsdyktighet til cyberangrep | Har dere opplevd cyberangrep?<br><br>Vet dere om noen del av deres arbeid som utgjør en cyberrisiko innenfor IT eller OT på fartøy?<br><br>Hvilke innarbeidede rutiner eller prosedyrer har dere for å sikre motstandsdyktighet til cyberangrep? |
| 7. Oppsummering | Synes dere at digitalisering i form av datainnsamling på fartøy totalt sett er positivt eller negativt med tanke på effektiv drift og forsvarlig cybersikkerhet på fartøy?<br><br>Er det noe du er spesielt opptatt av med hensyn til det vi har snakket om som du ønsker å legge til?<br><br>Om det ønskes å legge til noe: Hvorfor er dette viktig?<br><br>Gå igjennom og oppsummere det som er gjennomgått for å sikre at vi har forstått intervjupersonen riktig og om vi har fått med oss alt intervjupersonen vil tilføye.<br><br>Har vi forstått dere riktig?<br><br>Har dere noe mer å tilføye? |

| Intervjuguide 2 | Andre relevante aktører i maritim næring |
|---|---|
| **Hva vi ønsker å vite noe om** | **Forslag til spørsmål** |
| 1. Informasjon før intervjuet starter | Si litt om temaet for samtalen (bakgrunn, formål)<br><br>Forklar hva intervjuet skal brukes til, og forklar taushetsplikt og anonymitet<br><br>Spør om noe er uklart og om intervjupersonen har noen spørsmål<br><br>Informer og få samtykke til å starte opptak av intervju |
| 2. Personalia | Utdanning<br><br>Års erfaring<br><br>Nåværende stilling |
| 3. Grunnlag | Hva er deres forhold til digitalisering?<br><br>Hva er deres forhold til effektiv drift av fartøy?<br><br>Hva er deres forhold til forsvarlig cybersikkerhet? |
| 4. Bidrag | Hvordan arbeider dere med digitalisering i organisasjonen?<br><br>Hvordan arbeider dere med å fremme effektiv drift av fartøy i et organisasjonsperspektiv?<br><br>Hvordan arbeider dere med å bevare en forsvarlig cybersikkerhet i et organisasjonsperspektiv? |
| 5. Effektiv drift av fartøy<br><br>5.1. Generelt om effektiv drift av fartøy | Hvordan arbeider dere generelt for å fremme effektiv drift av fartøy?<br><br>Vil dere si at ansvaret om å fremme effektiv drift av fartøy ligger på sjøsiden eller landsiden? |
| Effektiv drift av fartøy<br><br>5.2. Teknologi som bidrar til digitalisering i form av datainnsamling på fartøy | Har dere oversikt over teknologiske verktøy som brukes for digitalisering i form av datainnsamling på fartøy?<br><br>Om dere har en oversikt:<br>Kan man dele disse teknologiske verktøyene inn i grupper eller kategorier etter verktøyets formål?<br><br>Leverer dere selv slik teknologi til rederi?<br><br>Hvilket utviklingspotensial ser dere i datainnsamlingsteknologien dere leverer til rederi?<br><br>Om dere leverer slik teknologi til rederi: Har dere fått noen tilbakemeldinger og eventuelt konkrete ønsker fra rederi om hvordan saker kunne vært gjort annerledes? |
| 6. Forsvarlig cybersikkerhet | Hvordan opplever du cybersikkerheten i maritim næring per. 2022? |

| | |
|---|---|
| 6.1. Oversikt over cybertrusler | Har dere en oversikt over hvilke cyberangrep som er mest utbredt i den maritime næringen?<br><br>Om dere har en oversikt:<br>Kan du gå litt i dybden på hvilke konkrete cyberangrep som er mest utbredt i den maritime næringen, eventuelt topp 3 typer cyberangrep mot fartøy og rederi? |
| Forsvarlig cybersikkerhet<br><br>6.2. Motstandsdyktighet til cyberangrep | Vet dere om noen del av deres teknologi som utgjør en cyberrisiko innenfor IT eller OT på fartøy?<br><br>Hvordan arbeider dere for å sikre at rederi som bruker av deres teknologi er best mulig sikret mot cyberangrep?<br><br>Har dere oversikt over hvilke typer cyberangrep som rederi blir mest sårbare for ved bruk av datainnsamlingsteknologi? |
| 7. Oppsummering | Synes dere at digitalisering i form av datainnsamling på fartøy totalt sett er positivt eller negativt med tanke på effektiv drift og forsvarlig cybersikkerhet på fartøy?<br><br>Er det noe du er spesielt opptatt av med hensyn til det vi har snakket om som du ønsker å legge til?<br><br>Om det ønskes å legge til noe: Hvorfor er dette viktig?<br><br>Gå igjennom og oppsummere det som er gjennomgått for å sikre at vi har forstått intervjupersonen riktig og om vi har fått med oss alt intervjupersonen vil tilføye.<br><br>Har vi forstått dere riktig?<br><br>Har dere noe mer å tilføye? |



NTNU

Kunnskap for en bedre verden