NECESSE | THE NORWEGIAN DEFENCE UNIVERSITY COLLEGE
THE ROYAL NORWEGIAN NAVAL ACADEMY | MONOGRAPHIC SERIES
VOLUME 3, ISSUE 2 - 2018

NECESSE

Militær navigasjon - teknologi og operative team

FHS/SKSK ARBEIDSMOTTO

Forsvarets høgskole / Sjøkrigsskolen,
en sentral- Kadett, elev og student fokusert skole - i FHS systemet.
Kompetent, fremtidsrettet, og relevant - for den militære profesjon.
En skole med mangfold blant ansatte og elever,
der akademia og maritim operasjonskunst går hånd i hånd - uadskillelig.
Uadskillelig - og fullt koblet til fellesoperative og allierte doktriner.

Necesse kommer i flere utgivelser hvert år. Skriftserien har en fagredaktør for hver utgivelse, samt en ansvarlig hovedredaktør. Necesse publiserer artikler som belyser problemstillinger relevante for operativ virksomhet. Under hovedoverskriften sjømilitær profesjonskompetanse har vi en tverrfaglig tilnærming med fem sjømilitære fagfelt: militær logistikk, maritime operasjoner, maritim militær teknologi, sjømilitært lederskap og militær navigasjon. Alle synspunkter i denne publikasjon står for forfatterens egen regning. Hel eller delvis gjengivelse av innholdet kan bare skje med forfatterens samtykke.

Necesse publiserer populærvitenskapelige artikler, som har som mål å formidle allerede publiserte vitenskapelige arbeider i et mer tilgjengelig format sammenlignet med originalarbeidene, samt vitenskapelige artikler som bidrar med ny og tidligere upublisert kunnskap.

Necesse er godkjent som et tverrfaglig vitenskapelig tidsskrift på Nivå 1 i publiseringssystemet. Retningslinjer som du må benytte hvis du ønsker å få publisert en faglig eller en vitenskapelig artikkel i Necesse er tilgjengelig på brage.bibsys.no – Sjøkrigsskolen. En vitenskapelig artikkel vil bli gjenstand for en dobbel, blindet fagfellevurderingsprosess før den blir vurdert for utgivelse. Andre typer artikler som ikke skal vurderes opp mot nivå 1 kriteriene vil bli vurdert og (eventuelt) godtatt av respektive fagredaktører. Necesse har et open access format, der denne og tidligere utgaver kan hentes på brage.bibsys.no – Sjøkrigsskolen. Her vil også alle vitenskapelige artikler være søkbare og lagt ut i PDF format.

Roar Espevik
Hovedredaktør Necesse

PB 5 Haakonsvern, 5886 BERGEN

ISSN 2464-353X
ISBN 978-82-93550-17-4 (elektronisk utgave)

Tittel: Necesse
The Norwegian Defence University College
The Royal Norwegian Naval Academy
Monographic series
Volume 3, Issue 2 - 2018
Undertittel: Militær navigasjon - teknologi og operative team
Hovedredaktør: Roar Espevik
Fagredaktør: Frode Voll Mjelde, Odd Sveinung Hareide
og Øystein Glomsvoll

Omslag og layout: Katrine Austgulen, HOS Grafisk
Foto fremside: Forsvaret
Foto bakside: www.scotlandnow.dailyrecord.co.uk

NECESSE

THE NORWEGIAN DEFENCE UNIVERSITY COLLEGE
THE ROYAL NORWEGIAN NAVAL ACADEMY

MONOGRAPHIC SERIES
VOLUME 3, ISSUE 2 - 2018

Militær navigasjon - teknologi og operative team

Andre utgivelser i skriftserien

Vol. 1	Issue 1	2016	Militær navigasjon - effektiv og troverdig
	Issue 2	2016	Realfag og teknologi for marineoffiseren
	Issue 3	2016	Mer for mindre
	Issue 4	2016	Endring = ledelse + verdsetting
Vol. 2	Issue 1	2017	Militær navigasjon - dagens teknologi for morgendagens krigføring
	Issue 2	2017	Sjømakt og sjømilitærutdanning
	Issue 3	2017	Realfag og teknologi for marineoffiseren
Vol. 3	Issue 1	2018	God når det gjelder?

Innhold

Innledning

Del 1

Sjøforsvaret som lærende organisasjon

Del 2

Militær praktisk navigasjon

Del 3

Teknologisk utvikling for effektiv navigasjon

Del 4

Bacheloroppgaver OM3 2018

Del 5

Gjengivelse av artikler publisert i andre tidsskrift

Del 6

Fagfellevurderte artikler

Forord

Militær navigasjon - teknologi og operative team

Maritim navigasjon blander både vitenskap og kunst. En god navigatør tenker både strategisk, operasjonelt og taktisk. Navigatøren planlegger hver reise nøye, og har inngående kunnskap om sin egen plan. Underveis i seilasen samler navigatøren informasjon fra en rekke kilder, evaluerer denne informasjonen, og bestemmer skipets posisjon. Navigatøren sammenligner deretter posisjonen med sin seilingsplan, sine operative forpliktelser, og sitt eget bestikk. En god navigatør forutser farlige situasjoner i god tid før de oppstår, og holder seg alltid i forkant av sin egen plan. Navigatøren er drillet og klar for øyeblikkelige inngripen og handlinger. Navigatøren leder og forener en rekke ressurser - elektroniske, mekaniske og menneskelige. Navigasjonsmetoder og teknikker varierer med type fartøy, ytre og indre forhold, samt gjeldende betingelser i situasjon og oppdrag. Noen viktige elementer for en vellykket seilas kan ikke læres fra en god bok innen nautikk eller en drivende dyktig lærer i et klasserom. Vitenskapen om navigasjon kan læres, men selve kunsten å navigere utvikles gjennom erfaring.

Den norske kystlinjen karakteriseres av langstrakte fjorder, holmer, skjær og et havområde som er kjent som et av verdens mest utfordrende med tanke på vær og vind. Store deler av året er denne kystlinjen mørklagt, mens det deler av sommeren er lyst døgnet rundt. De nordligste områdene er spesielt krevende, med lave temperaturer, sterk vind og åpne havstrekk som gir null beskyttelse fra havets og værets vrede. Dette gjør navigasjon i norske farvann spesiell og utfordrende, særlig for militær navigasjon.

Militære fartøy forventes å operere hvor som helst i den norske skjærgård med ekstremt kort reaksjonstid og i høye hastigheter, være «on scene and unseen» og kunne levere effekt i et mål med centimeters presisjon. Dagens militære fartøyer er avanserte skrog med høyteknologiske sensorer og integrerte systemer som skal fungere i høye hastigheter i krevende operasjonsområder. En militær navigatør må kunne utnytte ethvert potensial i fartøy, utstyr, besetning, vær og omgivelser til å skaffe seg en fordel i forhold til motparten. Militær navigasjon handler således om å bidra til operasjonell overlegenhet gjennom inngående kjennskap til navigasjonstekniske og menneskelige faktorer for optimal yteevne.
Riktig anvendelse av ny teknologi som støtter operasjoner i en felles operativ kontekst gir økt utnyttelse av våpen og sensorer, gir reduksjon i driftsavbrudd og øker Sjøforsvarets stridsevne.

Høyt kunnskapsnivå, robuste ferdigheter og gode holdninger skapes gjennom en grundig utdanning som kombinerer profesjonell veiledning med teori, simulator og praksis. Kombinasjonen mellom sertifiserende nautisk fagutdanning (bachelor) og praktisk militær navigasjon er helt nødvendig for at fremtidens militære navigatører skal få tilført kompetansen de trenger. Kontinuerlig faglig påfyll og nivåkontroller etter ferdig utdanning sørger for at Sjøforsvarets operative evne holder et høyt nivå.
Gjennom Sjøforsvarets Navigasjonskompetansesenter blir morgendagens navigatører rustet til å møte de utfordringene de treffer om bord på Sjøforsvarets fartøyer, og Sjøforsvarets fartøyer blir rustet til å møte utfordringene de treffer i nasjonale og internasjonale farvann.

Vi håper du finner innholdet i denne utgaven av Necesse engasjerende, og vi oppfordrer deg mer enn gjerne til å ta kontakt med forfatteren på epost eller stikke innom Navkomp for en faglig diskusjon for å videreutvikle militær navigasjon. Hvis noen av leserne ønsker å bidra til Necesse, så setter vi stor pris på eksterne relevante bidrag tilsendt redaksjonen.

God lesning!

Fagredaktører Necesse Militær Navigasjon;
Frode Voll Mjelde, Odd Sveinung Hareide
og Øystein Glomsvoll

Ord fra sjef Sjøkrigsskolen

Jeg er svært stolt over det arbeidet som gjøres med NECESSE. Skriftserien er helt i tråd med de oppdrag som er gitt til sjef Sjøkrigsskolen av sjefen for Forsvarets Høyskole (FHS). Oppdragene favner over undervisning, forskning og utvikling, og - formidling. NECESSE har kontakt med alle disse oppdrag, og for oss er det blitt en viktig og anerkjent kanal for formidling av funn, som igjen skal brukes innen undervisning.

Navigasjonskompetanse-senteret (NAVKOMP) er en svært viktig del av Sjøkrigsskolen; selv om senteret nå organisatorisk er lagt under Sjøforsvaret. Senteret har en krevende oppdragsportefølje, der leveranser til kadetter/elever utgjør en stor og viktig del. Det er NAVKOMP som står som faglig redaktør for denne niende utgivelse av NECESSE. Bidragene i denne utgaven spenner fra kadetters bacheloroppgaver, ansattes operasjonelle og vitenskapelige artikler, og peer-reviewed artikler fra eksterne bidragsytere. Det faglige er helt i tråd med det viktige og tette forholdet Forsvaret må ha mellom akademia og operasjonskunst.

Kvalitativ evne til å utføre operasjoner i det maritime domene er helt essensielt for sjøfartsnasjonen Norge. Sjøkrigsskolen holder en svært tett link til Sjøforsvaret, noe som igjen tilfører sjef FHS og FHS-systemet, herunder FHS/Sjøkrigsskolen, relevant og fremtidsrettet kunnskap om maritime doktriner og operasjonskonsepter. Dette påvirker igjen til rett strategi for maritim operativ kompetanseheving hos nye sjøkrigere.

Stor takk til bidragsytere til denne utgaven av NECESSE - da i særdeleshet til hovedredaktør KK/Dr. Roar Espevik for solid redaksjonelt arbeid gjennom lang tid, og til NAVKOMP sine fagredaktører for høy arbeidsmoral og profesjonell leveranse. NAVKOMP øker FHS/Sjøkrigsskolens helt nødvendige nærhet til Sjøforsvarets KNM Tordenskjold (KNMT), herunder det maritime krigføringssenteret (MKS), og til Warfare Areas som: ASuW, AAW, ASW, og EW. Vi får til en enda tettere symbiose mellom akademia og operasjoner.

Bård Eriksen. Foto: Truls Løtvedt

Til leserne - kos dere med denne utgaven av FHS/SKSK NECESSE.

Bård Eriksen
Kommandør
Sjef Sjøkrigsskolen

Ansatte ved Sjøforsvarets navigasjonskompetansesenter

Kommandørkaptein
Steinar Nyhamn

Avdelingsleder
steny@fhs.mil.no

Avdelingsleder for Sjøforsvarets Navigasjonskompetansesenter. Bakgrunn fra MTB som skipssjef og skvadronssjef. Masterutdanning innen nautikk fra University of Nottingham. Norsk representant i NATO arbeidsgruppe Navigasjon.

Orlogskaptein
Petter Lunde

Leder simulatorkontor
petlu@fhs.mil.no

Leder Simulatorkontoret. Utdannet ved Sjøkrigsskolen og studert ved NTNU i Trondheim. Har bakgrunn som NK på MTB og skipssjef på Minerydder. Jobbet ved Navkomp som lærer i 9 år med bruk av simulator i undervisning og forskning, prosjektleder ved anskaffelser av simulatorene og simulatorleder siden 2009 da simulatorkontorert ble opprettet.

Orlogskaptein
Frode Voll Mjelde

Fagleder Human Factors
frovo@fhs.mil.no

Jobber til daglig på Simulatorkontoret. Operativ bakgrunn fra Hauk klasse MTB, Sambandsteknisk bakgrunn fra Kystvakt og VTO på Minerydder. VOU og MSc utdanning fra US Naval Postgraduate School. Hovedfokus på Human Factors, Integrasjon av teknologi og personell i militære kampsystemer, CRM/BRM/ERM, Simulatorsystemer og Trening/øving av militære team. Norsk representant i NATO arbeidsgruppe Human Factors syntetiske miljøer.

Kapteinløytnant
Magne Bolstad

Hovedinstruktør simulator
mbolstad@fhs.mil.no

Hovedinstruktør ved Simulatorkontoret. Har bakgrunn fra Storm- og Hauk-klasse MTB og Skjold-klasse korvett i tillegg til tjeneste som skipssjef på skolefartøyene Hessa/Vigra. Har jobbet ved NavKomp i snart tre år som instruktør innen Praktisk Navigasjon, ECDIS-kurs, CRM/BRM/ERM –kurs og Militært Hurtigbåtkurs. Studerer for tiden ledelse ved NTNU i Ålesund.

Visekonstabel
Martin Frotvedt

Driftstekniker simulator
mfrotvedt@fhs.mil.no

Utdannet til Dataelektroniker ved SKSK/NAVKOMP etter 18 måneder som vernepliktig lærling og bestått fagprøve. Martin har utmerket seg i jobben som simulatortekniker og fikk i januar 2017 engasjement for 6 måneder på simulatorkontoret.

Orlogskaptein
Henning Sulen

Leder undervisningskontor
hensu@fhs.mil.no

Leder ved undervisningskontoret ved NavKomp. Sjøtjeneste på undervannsbåt, skolefartøy og fregatt med 2 deployeringer til STANAVFORLANT. Utdannet ved Sjøkrigsskolen og tok nylig masterutdanning innen nautikk ved University og Nottingham. Underviser i navigasjonsfag og militær navigasjon med fokus på å gjennomføre rutinene, teknikkene og metodene på en enkel måte.

Høgskolelektor
Hans Magne Gloppen

Lærer militær nautikk
hgloppen@fhs.mil.no

54 år, arbeidet som høyskolelektor i nautikk ved SKSK siden 2007. Bakrunn først fra fiskeri, senere som dekksoffiser offshore, surveyor - undervannsopersjoner offshore og som lektor på maritim teknisk fagskole. Maritim kandidat fra NTNU, utdannet dekksoffser kl 1 fra Fiskeriteknisk høgskule i Ålesund, praktisk pedagogisk utdanning fra høyskolen i Bergen.

Orlogskaptein
Lasse Hiis Bergh

Leder øvingskontor
lhbergh@fhs.mil.no

Leder for øvingskontoret. Sjøtjenestebakgrunn fra UVB, Fregatt og Kystvakt. 8 års tjeneste som skipssjef i Kystvakten. Tjenestgjorde ved Combined Maritime Forces i Bahrain fra juli 2015 til januar 2016.

Kapteinløytnant
Bjarne Haukås

Mønstringsoffiser
bjhaukas@fhs.mil.no

Mønstringsoffiser og faglærer Militær Praktisk Navigasjon (MPN) ved øvingskontoret. Hovedansvarsområde er mønstring og støtte til Sjøforsvaret i militær navigasjon. Bakgrunn fra Minedykkerkommandoen, Hauk klasse MTB og Skjold klasse kystkorvett. Tar for tiden master i "Management of Demanding Marine Operations" ved NTNU.

Orlogskaptein
Stein Egil Iversen

Leder navigasjonssystemkontoret
steiversen@fhs.mil.no

Leder Navigasjonssystemkontoret. Bakgrunn som elektrooffiser innen ubåtvåpenet samt tjeneste ved Sjøforsvarets Maskin- og elektroskole og Skole for Skipsteknikk og Sikkerhet. Hovedfokus støtte til Forsvarsmateriell innavigasjonsrelaterte prosjekter for å ivareta krav til militær navigasjon, samt opplæring av personell i Sjøforsvaret innen navigasjonssystemer/sensorer.

Kapteinløytnant
Øystein Glomsvoll

Lærer navigasjon
oglomsvoll@fhs.mil.no

Lærer i nautikk ved Sjøkrigsskolen. Bakgrunn som skipssjef på Stridsbåt 90 og navigatør på Skjold-klasse, Minerydder og Nornen-klasse IKV. Begynte på NAVKOMP høsten 2014 etter fullført MSc. in Positioning and Navigation Technology ved University of Nottingham.

Kapteinløytnant
Odd Sveinung Hareide

Fagleder elektronisk navigasjon
ohareide@fhs.mil.no

Fagleder Elektronisk Navigasjon, med fokus på integrerte navigasjonssystemer og elektronisk navigasjon i forbindelse med støtte til Sjøforsvaret og i undervisning samt navigasjonsrelaterte prosjekter. Bakgrunn fra MTB, Hauk- og Skjold-klasse. Utdanning fra University of Nottingham, gjennomfører for tiden en doktorgrad i nautikk ved NTNU og Universitetet i Tromsø.

Kapteinløytnant
Kåre Schiøtz

Fagleder navigasjonssystemkontor
kschiotz@fhs.mil.no

Fagleder Navigasjonssystemer. Gjennomfører undervisning og er ansvarlig for fagene navigasjonssystemer. Har også et spesielt fokus på radarteknologi. Bakgrunn fra MTB og skipssjef på Alta- og Oksøy-klassen.

Løytnant
Vibeke Thuesen

Instruktør
vthuesen@fhs.mil.no

Ansatt (midlertidig) ved øvingskontoret på Navkomp siden august 2017. Funksjon som instruktør i Militær Praktisk Navigasjon (MPN). Uteksaminert ved Sjøkrigsskolen sommeren 2013. Bakgrunn fra KV stab og Fregatt.

Kapteinløytnant
Anders Fiskerstrand

Lærer navigasjon
afiskerstrand@fhs.mil.no

Ansatt ved undervisningskontoret på Navkomp siden januar 2018. Uteksaminert ved Sjøkrigsskolen i 2005. Operativ tjeneste på fregatt 2005-2010 og 2014-2018, samt hovedinstruktør navigasjon ved fregatt treningssenter 2010-2012. Permisjon fra Sjøforsvaret i perioden 2012-2014, og jobbet da som styrmann på seismikk hos Eidesvik Offshore.

DEL 1

Sjøforsvaret som lærende organisasjon

Trender etter grunnstøtinger i Sjøforsvaret

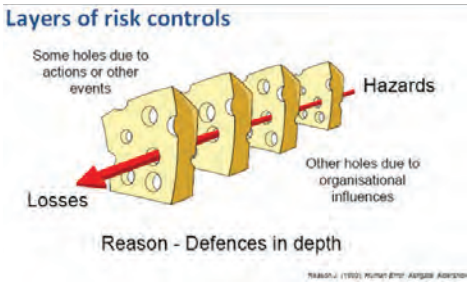
Steinar Nyhamn

Sammendrag

Etter 2004 har det vært 13 grunnstøtinger eller grunnberøringer hvor det har blitt besluttet å nedsette kommisjon. Historisk har fokuset for kommisjonen dreiet fra å fastslå menneskelig svikt til å identifisere faktorer som sammen førte til den uønskede hendelse. Det viser seg at de aller fleste kommisjonsrapporter identifiserer de menneskelige faktorene gruppetenkning og complacency som svært viktige faktorer, noe som også er gjengangere i sivil skipsfart.

Innledning

I 100% av grunnstøtingen undersøkt i perioden er det identifisert menneskelig svikt som avgjørende eller viktig grunn til hendelsen. I sivilt maritimt miljø er det ca. 80% av hendelsene som ikke lister teknisk svikt som en direkte årsak. Analyser indikerer at menneskelig feil er direkte årsaksfaktor i 80% av alle uhell. Komplekse teknologiske miljøer er i 50-60% av uhell oppført som indirekte årsak. Før rundt år 2000 kunne det virke som om hovedhensikten med kommisjoner i Sjøforsvaret var å finne en ansvarlig som eventuelt kunne refses. I tiden etter dette har hovedfokus til kommisjonene blitt å finne hva som førte til at det ble menneskelig svikt.



Bilde 1 Swiss cheese modellen

Dette har krevd at deltakerne har kunnskap innen feltet og har vært villige til å bruke den i analysene. Noe av denne kunnskapen har kommet gjennom økt fokus på nettopp mellommenneskelige forhold som bla er formalisert gjennom Crew Resource Management (CRM) kurs. Det er imidlertid varierende systematikk ila disse årene som vanskeliggjør identifisering av trender. Likevel står noen trender frem. Denne artikkelen vil ta for seg noen av hovedområdene som har vært gjengangere i de fleste rapportene.

Faktorer

Gjennom innsamling av data er kommisjonens viktigste oppgave å finne relevante faktorer som kan tenkes å kaste lys over årsaken til hendelsen og som det kan dras lærdom av. Slike faktorer kan generelt inndeles i fire hovedgrupper: menneskelige, oppgaverelaterte, systemtekniske eller miljømessige faktorer. Dette inkluderer også forholdet mellom menneske og maskin (MMI). Enkeltstående faktorer er for seg selv ofte «uskyldige» og ikke nok til at de fører til en hendelse eller reaksjon, men kan gi en forklaring i en større sammenheng. Dette fenomenet er ofte forklart med «Swiss cheese» modellen, Bilde 1, som viser hvorledes egne og andres beslutninger (hendelser) over tid fører til et tap eller økt risiko for en uønsket hendelse.

Utfordringene for en kommisjon er at det er vanskelig å sette grenser hvor langt fra kjerneområdet (hovedårsaken) det er hensiktsmessig å trekke inn faktorer i analysen. Et eksempel på dette kan være at det kommer frem en svakhet i rutiner for overlevering innen maskindetaljen. Dette kan være alvorlig; det er veldig vanskelig å knytte til hendelsen og de viktigste faktorene. Dog er det i utgangspunktet viktig å ikke forkaste noe da det ila analysen kan vise seg å være et element som hadde «hull» som ikke stoppet faren for potensiell skade. Hvis det har vært tvil om relevans, har løsningen vært å nevne elementene, men samtidig slå fast at de ikke hadde noe relevans for den spesifikke hendelsen.

Menneskelige faktorer

Menneskelige faktorer er individrelaterte faktorer som anses relevante i ulykkesvurdering. Kognitive egenskaper kan deles inn i midlertidige faktorer (forventninger, opplevelser, konsekvensanalyse) og mer varige faktorer (oppmerksomhet, kunnskapsnivå, utdanning og erfaring). Tilsvarende kan fysiske og psykiske egenskaper beskrives.

Oppgaverelaterte faktorer

Herunder hører faktorer som kan samles under prosedyrer, oppgavekrav og oppgave type.

Systemfaktorer

Slike faktorer deles primært inn i MMI (Man-Machine Interface) og systemstatus (feilfunksjon).

Miljømessige faktorer

Dette omfatter det fysiske arbeidsmiljøet og organisasjonsmessige faktorer, herunder sikkerhetskultur, vaktordninger, grad av tilsyn og veiledning.

Organisatoriske faktorer

Faktorer som har med forholdene rundt arbeidsplassen kan være med på å føre til menneskelig svikt. Dette kan for eksempel være manglende tilrettelegging for de oppgaver som pålegges eller krav som er med på å øke risiko i arbeidssituasjonen. Organisatoriske faktorer kan være:

- Eksterne (budsjett, etc.)
- Interne (vaktlister, etc.)
- Usikker instruksjon
- Utilstrekkelig opplæring
- Mangelfull kjennskap til utstyr, begrensninger/ virkemåte
- Tilstand på personell og utstyr
- Perfekte tilstander, uthvilt og oppøvd
- Dårlig stemning, trøtthet, utslitt, lav kompetanse
- Design av arbeidsplassen
- Usikre hendelser
- Prosedyrefeil
- Regelbrudd
- Forberedelser (mangel på avklaringer)

Complacency og Gruppetenkning

I samtlige rapporter etter 2004 er det pekt på menneskelige faktorer som direkte årsak eller vesentlige bidragsytere. Alle rapporter inneholder også organisatoriske faktorer hvor de mest fremtredende er manglende systemkunnskap, dårlig design og prosedyrebrudd. Dette vil ikke bli utredet nærmere i denne artikkel. De to mest fremtredende menneskelige faktorene er *complacency* og gruppetenkning og blir bearbeidet mer i dybden i denne artikkelen.

Det er vanskelig å finne et godt norsk ord for *complacency*, men ordet behagelighetsfølelse og tilfredshetsfølelse har blitt brukt. Kommisjonsrapporten etter KV Andenes beskriver følgende:

> *«Når operatører eller team blir så godt kjent med en oppgave at utførelser går på autopilot, så synker også årvåkenheten og evnen til å oppdage avvik og kritiske forhold som påvirker ytelse og utførelse. De undervurderer kompleksiteten i å gjøre ting samtidig. Complacency kan også komme av understimulering og kjedsomhet. Elementer som: «Følg lederen» og «Slik gjør vi det her» karakteriserer en slik gruppe.*

Flere rapporter og erfaringer fra mønstringer understreker dette. Det er liten interesse for å sette seg inn i nytt utstyr og utforske nye muligheter samt at det sjeldent stilles spørsmål om «hvorfor». Operatørene har kommet inn i en sedvane og har i liten grad kritisk sans som kunne ført til kreativitet som igjen kunne påvirket effektivitet og utvikling.

Et eksempel på dette er fra et fartøy som klagde på at det gikk en alarm med jevne intervaller. Denne var svært irriterende og utkikken hadde fast jobb med å nullstille den. Prosedyren var etablert og hadde pågått i flere år: det var blitt en vane. Ila disse årene tok aldri noen initiativ til å finne ut hvorfor alarmen kom og hva som kunne bli gjort for å få den bort. Det tok en utenforstående (ikke ekspert) 5 min å fjerne denne.

Et annet eksempel er fra et fartøy som hadde et utstyr om bord som de ikke hadde fått typekurs på. Svaret på hvorfor de ikke brukte det var godt innarbeidet; «vi har ikke kurs». De var tilfreds med dette, og det ble ikke gjennomført noe initiativ til å lære seg utstyret eller utforske det videre. Dette måtte de ha gjort uansett etter et typekurs.

Britiske Marine Accident Investigation Branch (MAIB) har hatt sammenfallende erfaring. I nesten alle undersøkelser av grunnstøtinger og kollisjoner blir complacency angitt som en vesentlig faktor. I et forebyggende flygeblad (MAIB, 2008) utgitt av MAIB til skipsindustrien i 2008 ble følgende påpekt:

> *"Complacency continues to be a recurring safety issue in accidents investigated by the MAIB. Shipowners should recognise the risks posed by complacency and ensure that their vessels operate with effective bridge teams at all times."*

Samhandling på en kompleks plattform med kompliserte oppgaver under varierende forhold kan være krevende. Det kan være utfordringer av positive og negative art. En av disse utfordringene er kalt gruppetenkning (Flin, O'Connor, & Crichton, 2009). På Sjøkrigsskolen legges det stor vekt på kadettenes evne til å kunne løse krevende oppdrag i team. Grunnen til dette er at grupper eller team forventes å inneha en samlet økning i kognitive ressurser og de kan dermed forventes å utføre oppgaver mer effektivt. Kadettene blir trent i for eksempel å observere hverandres ytelse, sammenfatte kunnskap, anbefale strategier og løsninger, tilby støtte. De utvikler god innsikt i væremåter, holdninger og den enkeltes styrker og svakheter. Dette skal i teorien redusere total arbeidsbelastning og gi gruppen en transparent utøvelse av komplekse arbeidsoppgaver. Det er imidlertid komplekst både i teorien og i praksis. Dette kan føre til det motsatte; dysfunksjonelle grupper som i verste fall ikke fungerer i en krisesituasjon.

Kommisjonsrapporten etter KV Andenes (KV Andenes, 2013) beskriver også gruppetenkning:

> *Dessverre kan grupper også møte utfordringer i beslutningstakingsprosesser, rollefordeling og koordinering av oppgaver. Gruppetenkning kan oppstå i en gruppe når rasjonelle valg undertrykkes for å opprettholde gruppens standarder og sedvaner. Medlemmer unnlater dermed å dele informasjon som burde vært relevant til en beslutning eller utførelse, men deler kun informasjon som de anser passende til gruppens typiske vaner.*

Som det fremkommer er det sammenheng mellom disse begrepene selv om de er forskjellige. *Complacency* har best grobunn i en gruppe som gjør fastlagte arbeidsoppgaver men som også skal være i stand til å gjøre andre innovative oppgaver. At det er mange grupper, både formelle og uformelle, gjør ikke det enklere å oppdage og motarbeide dette. Sjøforsvaret med sin «lean manning» bemanningspolitikk er helt avhengig av at grupper er effektive på alle nivåer, men det gjør det heller ikke enklere at de samme personene har mange forskjellige roller.

Oppsummering og veien videre

Den analyserende måten å produsere kommisjonsrapporter på har utvilsomt gitt en innsikt i faktorer som påvirker uønskede hendelser i Sjøforsvaret. Innenfor menneskelige faktorer har *complacency* og gruppetenkning skilt seg ut som en trend. Det har også vært tilsvarende utvikling i sivil maritim sektor.

Det er lett å hevde at vi lærer for lite av kommisjonserfaringer, men det er nok en sannhet med modifikasjoner. Som helhet har nok erfaringen fra kommisjoner ført til endringer som reduserer risiko. Tar man utgangspunkt i kortere perioder kan det imidlertid hevdes at vi ikke har lært noe. Eksempel på det siste kan være MTB våpenet som hadde 5 grunnberøringer på ett år eller Kystvakten som hadde flere grunnstøtinger ila av noen få år uten at det ble gjort noen vesentlige tiltak. Når rapportene beskriver de samme faktorene og anbefalingene, er det fristende å konkludere med at det ikke har noen effekt. Man kan imidlertid hevde at vi generelt er for dårlig til å lære og endre adferd. Kystvakten «våknet» imidlertid i 2013 og har gjort stor fremgang i de seinere år. Det er nok ikke mangel på vilje, men når det handler om endring av rutiner og endring av holdninger, støter man på komplekse utfordringer. Selv ledelsen som skal stå for endringene kan være påvirket av en form for *complacency*; «vi har jo alltid gjort det slik», «det gikk jo bra når jeg var om bord» osv. Der erfaringene med sikkerhet har hatt effekt er i utviklingen av faget militær navigasjon. Publikasjonen SNP 500 gir føringer innenfor disse områdene og temaet er inkludert i pensum på Sjøkrigsskolen gjennom både teori og praksis.

Sjef Sjøforsvaret og Sjef Marinen har også vist stor interesse for temaet og har indikert at det skal settes inn tiltak for å få ned risikoen i fremtiden. Forslag til tiltaksliste er oversendt Sjef Marinen pr mars 2018 så er det bare å krysse fingene for at det blir tilstrekkelig oppfølging og at ledelsen ikke går i complacency fellen.

Referanser

1. Marine Accident Investigation Branch (MAIB). «Safety flyer to the shipping industry»; 2009.
2. Forsvarets operative hovedkvarter (FOH) *Kommisjonsrapport etter grunnstøting KV Andenes*; 2013.

Rapportering av uønskede hendelser vedrørende navigasjon i 1. Fregattskvadron

Henrik Steffensen og Marte Aas

I januar 2017 går KNM Otra på grunn etter å ha stevnet Saltskår lykt for lenge. Fire år tidligere blir KV Andenes stående på grunn ved Rødbergodden. Denne teksten er en redigert utgave av en bacheloroppgave skrevet ved Sjøkrigsskolen våren 2017 og omhandler rapportering av uønskede hendelser vedrørende navigasjon i 1.Fregattskvadron.

Rapporteringsregimet i Sjøforsvaret eksisterer i hovedsak for å kunne redusere sannsynligheten for at uønskede hendelser skal gjenta seg. Gjennom rapportering kan fartøy lære av andre og egnes erfaringer og potensielt unngå lignende uønskede hendelser i fremtiden. For at dette skal fungere kreves det at uønskede hendelser blir rapportert. Fra 2009 til 2017 er det registrert 19 uønskede hendelser vedrørende navigasjon i 1. Fregattskvadron. De fleste innrapporterte uønskede hendelsene som ble rapportert i denne tidsperioden omhandlet feil på brosystem, ikke menneskelig svikt. Tilnærmet ingen av hendelsene som ble rapportert var uønsket hendelse som direkte konsekvens av navigasjon. Dette reiser spørsmålet: Er navigatørene veldig gode til å navigere – eller er de dårlige til å rapportere?

Følgende er oppgavens problemstilling: *"Eksisterer det underrapportering av uønskede hendelser vedrørende navigasjon i 1. Fregattskvadron?"*. For å finne svar på problemstillingen ble en spørreundersøkelse med 28 spørsmål utarbeidet. Metoden som ble brukt i oppgaven er et ekstensivt design. Dette ble valgt for å undersøke i bredden, og for å kunne se etter tendenser i skvadronen. Undersøkelsen ble sendt til nåværende og tidligere navigatører som fortsatt tjenestegjør ombord, og skipssjefer i skvadronen. Spørsmålene er utarbeidet for å kartlegge om det eksisterer underrapportering, og eventuelt årsaker til dette. Det er viktig understreke at halvparten av utvalget har svart på undersøkelsen.

I bacheloroppgaven presenteres relevant teori for begrepene risiko, sikkerhet og sikkerhetskultur. Videre presenteres high reliability-organization, normal accidents-teorien, organisasjonskultur og læringsteori. I denne teksten er det valgt å presentere et utdrag av de viktigste teoriene fra oppgaven.

Sikkerhetskultur

I Sjøforsvaret har man jobbet med å implementere et helhetlig system for styring av sikkerhet. For å oppnå dette må det etableres en god sikkerhetskultur, hvorpå en viktig del av denne kulturen er å kartlegge og rapportere uønskede hendelser (SST 2013, 14). Målet med Sjøforsvarets sikkerhetsfilosofi er *"effektiv og sikker operativ evne og slagkraft basert på et fungerende sikkerhetsstyringssystem og god sikkerhetskultur"* (Sjøforsvarsstaben

2013, 7). Tanken bak rapportering er å lære av de hendelser og nesten-ulykker som oppstår. Gjennom å lære av allerede oppståtte hendelser og de erfaringer andre pådrar seg, skal man unngå at lignende hendelser skjer igjen.

Rapporterende kultur

Skal man oppnå en god sikkerhetskultur må man legge til rette for og oppnå en rapporterende kultur. En rapporterende kultur avhenger av velvillig deltagelse blant de ansatte som er i direkte kontakt med farene. Det fordrer at de er villige til å rapportere feil, hendelser og avvik. Det er et ledelsesansvar å legge til rette for en rapporterende kultur. Dette gjelder også i Forsvaret, og er forankret i *direktiv - krav til sikkerhetsstyring i Forsvaret*, undertegnet av FSJ Harald Sunde (Forsvarsstaben 2011). Å få ansatte i en organisasjon til å rapportere feil kan være en vanskelig oppgave, spesielt når man skal rapportere egne feil. Menneskelige reaksjoner på å begå feil varierer, men tilståelse står sjeldent øverst på lista (Reason 1997, 196). Fokuset man ønsker, er at rapporter skal bidra til å fremme et trygt arbeidsmiljø, fremfor på straff og skyld (Reason 1997, 196). Skal man få de ansatte til å rapportere må det være enkelt å rapportere, i tillegg må de ha kunnskapen og vite hvordan dette faktisk gjøres (Reason 1997, 202).

Organisasjonskultur

En fregattbesetning består av en organisasjon sammensatt av mennesker som må samhandle for å kunne løse oppdrag. Ifølge Henning Bang er kulturen i organisasjonen svaret på hvorfor noen organisasjoner er suksessfulle i sitt arbeid, mens andre mislykkes (2011 Bang, 14). Henning Bang bruker følgende definisjon på organisasjonskultur: *"Organisasjonskultur er de sett av felles verdier, normer og virkelighetsoppfatninger som utvikler seg i en organisasjon når medlemmene samhandler med hverandre og omgivelsene*" (2011 Bang, 23).

Verdier i denne sammenheng skal forstås som det medlemmene i organisasjonen etterstreber. Verdier kan deles inn i forfektede verdier og bruksverdier. Forfektede verdier er typiske slagord som kan leses på en plakat. For Forsvaret vil dette typisk være respekt, ansvar og mot. Bruksverdier er de verdier som faktisk baserer seg på utøvde handlinger. Det kan være på grunnlag av hva som gir status i gruppen, eller hva ledelsen faktisk belønner, både formelt og uformelt. Det er disse verdiene som kjennetegner organisasjonskulturen (2011 Bang, 47).

Normene sier noe om hvordan medlemmene bør oppføre seg i forhold til regler og hverandre. Det definerer akseptable og uakseptable holdninger og handlinger. Normer kan videre knyttes opp mot verdier da normer sier noe om hvordan man konkret skal handle for å oppfylle verdiene (2011 Bang, 51).

Drøfting

I oppgaven ble data fra undersøkelsen behandlet og analysert i statistikkprogrammet IBM SPSS. Det ble gjennomført en korrelasjonsanalyse for å se etter sammenhengen mellom de ulike spørsmålene. I tillegg til en korrelasjonsanalyse ble det på spørsmål med høy korrelasjon gjennomført en regresjonsanalyse. Denne sier noe om hvor tilfeldig sammenhengen (korrelasjonen) er. Oppgaven drøfter kun funn med høy signifikans, altså ikke tilfeldig sammenheng. I denne teksten har vi valgt et utdrag av drøftingen.

Studien viser en sterk sammenheng mellom opplæring av nye navigatører og om man opplever en god rapporteringskultur ombord. På spørsmål om navigatøren har fått opplæring i hvordan man skal rapportere uønskede hendelser vedrørende navigasjon svarer bare 33% at de har fått opplæring i hvordan de skal rapportere uønskede hendelser. Og kun 22% er enige i at nye navigatører får opplæring i rapportering. Dette er et relativt lavt tall, noe som kan føre til underrapportering.

Hvis man skal oppnå læring basert på rapporter må disse komme tilbake til brukeren og gjennomgås. Dette fordrer at man har rapporter å gjennomgå. Skal navigatøren bruke tid på å rapportere en uønskede hendelser, fordrer det at vedkommende kjenner til formålet og vet hvorfor uønskede hendelser skal rapporteres. Bare 55% sier at de kjenner til formålet med rapportering. Kanskje ikke så rart når det kun er 33% som sier at de har fått opplæring i hvordan de skal rapportere. Rapportering er ikke noe man i utgangspunktet blir pålagt, men er noe man frivillig kan velge å gjøre. Dersom navigatørene skal bruke tid på å fylle ut og sende inn rapporter forutsetter dette at de har fått opplæring og kjenner formålet.

Ledelsen ombord må legge til rette for at tidligere innsendte rapporter gjennomgås slik at man lærer av disse hendelsene. 28% av de spurte som sier seg enige i at rapporter fra andre fartøy blir systematisk gjennomgått i egen besetning. Ved en slik gjennomgang, hvis den oppleves nyttig, vil man kunne reflektere over hva som har skjedd og senere gjenkjenne situasjoner og forhåpentligvis unngå at lignende hendelser gjentar seg.

Fra resultatene i spørreundersøkelsen ser man at hele 94% av respondentene forstår viktigheten av å rapportere uønskede hendelser vedrørende navigasjon. At et så høyt antall av respondentene forstår viktigheten av å rapportere, kan komme av ledelsens uttalte forfektede verdier. Dette gir et betydelig potensial for oppnå en god sikkerhetskultur. I utgangspunktet kan man anta at en organisasjon som ser viktigheten av å rapportere, blir en rapporterende kultur, men det er ikke nødvendigvis

riktig. Analysen viser at det ikke er noen sammenheng mellom å forstå viktigheten av å rapportere, og at man opplever en god rapporteringskultur. Dette kan komme av at det ikke er nok reelt fokus og oppfølging fra ledelsens side, eventuelt at det ikke belønnes eller gis noen status i organisasjonen for å rapportere (2011 Bang, 47).

Ser man nærmere på spørsmålet "Jeg har i tjeneste opplevd uønsket hendelse vedrørende navigasjon som burde vært rapportert, men som ikke ble det", er hele 40% enige i påstanden. Fra dette resultatet vil det være nærliggende å anta at det eksisterer underrapportering av uønskede hendelser vedrørende navigasjon i 1. Fregattskvadron. 28% svarer at de ikke vet. Dette kan være et resultat av at det ikke eksisterer en felles anerkjent og konkret grense for hva som skal rapporteres og ikke. Dette stiller dermed større krav til ledelsen om å sette føringer for hva som skal rapporteres og ikke.

Konklusjon

Målet med oppgaven var å finne svar på problemstillingen: *Eksisterer det underrapportering av uønskede hendelser vedrørende navigasjon i 1. Fregattskvadron?* På grunn av relativt få antall respondenter velger vi i denne oppgaven å ikke konkludere, men å bruke svarene til å peke på tendenser i skvadronen.

Studiens funn peker mot at de fleste navigatørene kjenner til viktigheten av å rapportere uønskede hendelser, men de mangler opplæring i hvordan dette gjøres, videre er det mange som ikke kjenner til formålet med rapportering. Det ser heller ikke ut til at det settes av mye tid til gjennomgang av hendelser.

Det vil ut ifra funnet om ledelsens fokus, være rimelig å anta at ledelsen fokus på rapportering påvirker besetningens rapporterings- og organisasjonskultur. Studien viser at de navigatørene med ledere som har fokus på, og oppfordrer til rapportering, også er de navigatørene som opplever en god rapporteringskultur ombord. Ut i fra funnene i studien er NAVKOMP også en viktig bidragsyter gjennom å oppfordre til at hendelser rapporteres.

Frykt for straff ser ikke ut til å være en overveiende årsak til hvorfor navigatørene unnlater å rapportere hendelser. Det kan derimot se ut som om at det mangler en konkret og forståelig grense for hva som skal rapporteres, da definisjonen på uønsket hendelse er lite gripbar.

Basert på funnene hvor respondentene svarer at de har unnlatt å rapportere og på bakgrunn av rapporteringsstatistikken, er det indikasjoner på at det eksisterer underrapportering av uønskede hendelser vedrørende navigasjon i 1. Fregattskvadron. Denne hypotesen blir styrket av oppgavens drøfting, hvor det er mangelfulle forhold basert på teorigrunnlaget, for at skvadronen skal ha en rapporterende kultur.

Referanser

Bang, Henning 2011. *Organisasjonskultur*. Oslo: Universitetsforlaget AS.

Forsvarsstaben 2011. *Forsvarssjefens direktiv – Krav til sikkerhetsstyring i Forsvaret*, Oslo: Forsvarsstaben.

Reason, James 1997. Reason, James. *Managing the risk of organizational accidents.* Surrey, England: Ashgate publishing company.

Sikkerhetsinspektør i Sjøforsvaret 2016a. *Prosedyre for rapportering og registrering av uønskede hendelser og tilstander i Sjøforsvaret.* Bergen: Generalinspektøren i Sjøforsvaret.

Sikkerhetsinspektør i Sjøforsvaret 2016b. *Instruks for hendelseshåndtering i Sjøforsvaret.* Generalinspektøren i Sjøforsvaret.

Sjøforsvarsstaben 2013. Sjøforsvarsstaben. *Håndbok sikkerhet.* SSTP, avdeling for Sikkerhet og Kvalitet (SST ASK).

Stikkholmen, Bjørn-Ove 2012. Stikkholmen, Bjørn-Ove. *Sikkerhetskultur i Sjøforsvaret.*

Innføring av CRM/BRM i SNP-500

Frode Voll Mjelde

Sammendrag

Effektiv og sikker militær navigasjon oppnås gjennom navigasjonstekniske ferdigheter, utstyrskompetanse og evne til samspill og samhandling. Crew Resource Management (CRM) fokuserer i så måte på menneskelige faktorer i lederskap og lagarbeid for å øke effektivitet og til å forebygge uhell og ulykker i Sjøforsvaret og andre våpengrener.

SNP-500 er Forsvarets reglement for militær navigasjon på Forsvarets sjøgående fartøy, og fokuserer i hovedsak på navigasjon og broteamet. Denne artikkelen beskriver innføringen av CRM prinsipper i SNP-500 og vil omhandle retningslinjer for effektiv samhandling og kommunikasjon på bro; som i maritim sammenheng omtales som Bridge Resource Management (BRM). Sjøforsvarets primære hensikt med fokuset på menneskelige faktorer er å gjøre broteamet bedre rustet til å jobbe i team, forhindre misforståelser og uhell, og å sikre effektiv og taktisk navigering.

Militær navigasjon omfatter både navigasjonstekniske og menneskelige faktorer. Figur 1 illustrerer omfanget av faktorer som en militær navigatør må forholde seg til.

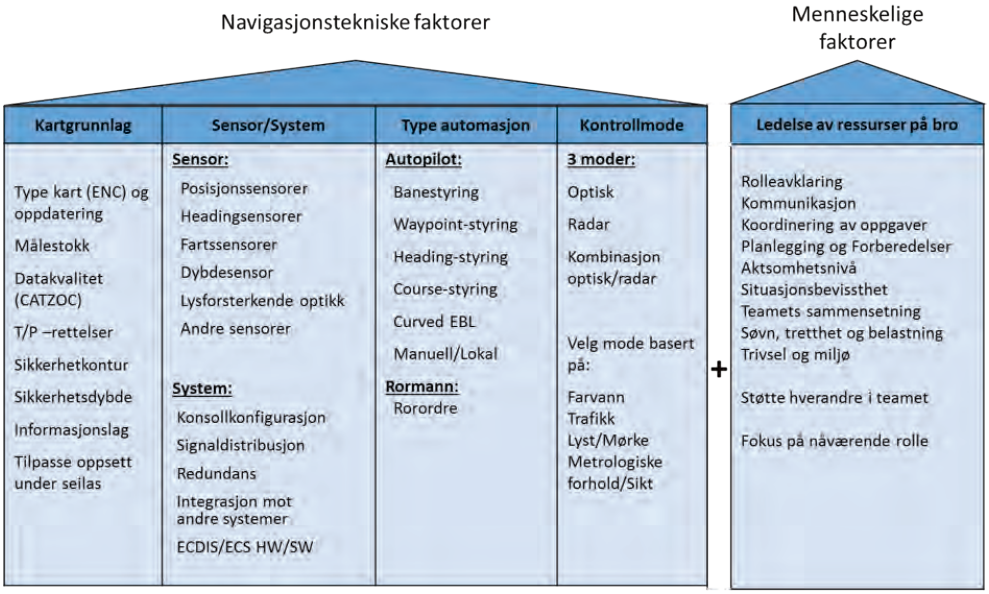
SNP-500 er en samling av regler med innledende forklaring hvor emner starter med en beskrivelse og ender opp med en regel, hvor den innledende forklaringen underbygger reglene. Den nye utgaven av reglementet vil omtale krav til menneskelige faktorer i et eget kapittel for CRM/BRM, med forventet publisering i Forsvarets interne arkiv (FOBID) i løpet av tredje kvartal 2018.
CRM/BRM kapittelet beskriver emner for ledelse av ressurser på bro som illustrert i figur 1. I den grad det har vært mulig er det referert til annen relevant informasjon og forskning som kan gi utdypende forklaringer.

Rolleavklaring

God rolleavklaring øker teamets effektivitet og evne til måloppnåelse. Studier av havarier og ulykker har identifisert mangelfull rolleavklaring som en av de vanligste grunnene til teamsvikt, som igjen har vært medvirkende eller direkte årsak til tap og skader av personell og materiell (Flin, O'Connor, & Crichton, 2008). Klar og tydelig rolleavklaring er derfor meget viktig både for teamets standard operasjonsmønster og for nye eller spesielle operasjoner.

Det er dokumentert at team presterer dårligere når det kommer inn et nytt medlem (Cannon-Bowers & Salas, 1998). I Sjøforsvaret skjer dette til stadighet når vi låner personell fra andre fartøy eller treningssentre, eller når personell rulleres ved beordringsoppgjør. Ved ankomst av nytt personell som skal inn i broteamet må disse gjøres oppmerksom på fartøyets krav og forventninger til etablerte rollemønstre.

Dersom sjefen skal inngå i broteamet må han/hun være innforstått med rollemyndighet og sin betydelige påvirkning på teamets adferd. Misforståelser har vist seg å oppstå når sjefen kommenterer eller korrigerer utførelsen av navigasjon uten å formelt overta ansvaret. Dette medfører usikkerhet i broteamet om hvem som har ledelsen, og navigasjonssikkerheten reduseres. Sjefen må derfor tydelig kommunisere hvilken rolle som bekles.



Figur 1, Faktorer som påvirker navigatører i Forsvaret (Sjøforsvarets Navigasjonskompetansesenter, 2018)

Regel – Rolleavklaring

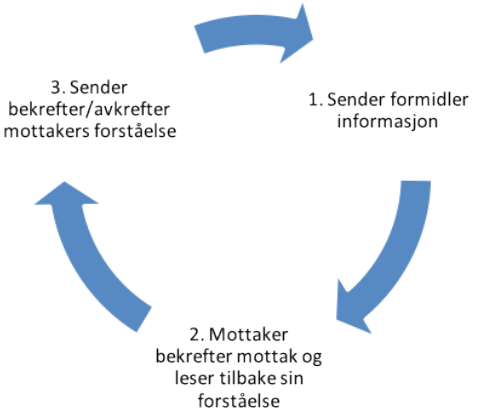
- Hver fartøysklasse skal definere hvilke roller som skal besettes i et broteam for alle kjente operasjonsmønstre.
- Det skal defineres ansvarsområder og tilkjennegjort hvilken myndighet rollen har på vegne av ledelsen.
- Det skal defineres hvilke kunnskaper, ferdigheter og holdninger som kreves og forventes til de ulike rollene.
- Vaktsjef er leder av broteamet selv om sjefen er på bro, med mindre annet er eksplisitt kommunisert etter rutiner for overtakelse.

Kommunikasjon

Kommunikasjon er utveksling av informasjon, tilbakemeldinger og respons (Fig 2), og er en viktig aktivitet i koordinering mellom teamets medlemmer for å oppnå sine mål. Kommunikasjonsproblemer er kjent for å bidra til misforståelser, uhell og ulykker i nær sagt alle yrker. Det betyr at god og riktig kommunikasjon innad i broteamet er en meget viktig faktor for oppgaveforståelse og oppdragsløsning. Alle i broteamet må forstå viktigheten av konkret og utvetydig ordregang og kommunikasjon.

Som mennesker legger vi mer vekt på tonefall og kroppsspråk (ikke-verbale tolkninger) enn vi gjør på hva som faktisk blir sagt. Kroppsholdning og måten man snakker til andre mennesker på i teamet har vist seg å bety veldig mye for samspillet i team. Derfor er det viktig at alle tenker gjennom sin væremåte og fremtreden når man skal fungere i et broteam.

Eksempler som fremmer kommunikasjon i team kan være: åpenhet, aktiv lytting, tydelig innhold, tydelig fremføring, timing (rett informasjon til rett tid, og i passelig mengde).



Figur 2, Closed-loop communication

Lukket kommunikasjonssløyfe (closed-loop communication) er en kommunikasjonsteknikk som øker sannsynligheten for at informasjon blir klart og konsist overført, mottatt, og riktig forstått (Wilson, Salas, Priest, & Andrews, 2007). Den foregår i en tre-trinns sekvens hvor informasjonen overføres fra avsenderen, blir mottatt og lest tilbake av mottakeren og bekreftes/korrigeres dernest av avsenderen (Salas, Sims, & Burke, 2005).

Regel – Kommunikasjon
- Broteamet skal utveksle informasjon klart og tydelig og med tilbakemelding og respons.
- Navigasjonsordrer skal følge Sjøforsvarets fastsatte prinsipper.

Koordinering av oppgaver

Koordinering av oppgaver innebærer at teamets leder eksplisitt kommuniserer delegering av oppgaver, samt hvilke prioriteringer som gjelder. Medlemmer av broteamet får dermed en klar og tydelig oppgavefordeling som definerer hvordan de forholder seg til oppdraget. Uttalte prioriteringer øker oppmerksomheten for tildelt oppgave og minsker mulighetene for misforståelser og antakelser (Serfaty, Entin, & Johnston, 1998).

Team som evner til å sette av tid til å holde alle oppdatert på prioriteringer og situasjonsbilde øker teamets situasjonsforståelse og evne til måloppnåelse.

Regel – Koordinering av oppgaver
- Broteamet skal delegere og prioritere oppgaver basert på teamets ferdigheter og oppdragets art.

Planlegging og forberedelser

Kritiske situasjoner og navigasjonsuhell har oppstått på grunn av innblanding i navigasjonen av personell som ikke har vært forberedt på seilas i det aktuelle farvann. Planlegging og gode forberedelser bedrer mentale modeller, gir mer overskudd og øker sannsynligheten for at navigatøren evner å oppfatte farer og avvik i omgivelsene (Orasanu, 1995).

Blant annet vil Los om bord kreve særskilt oppmerksomhet. Det må avtales nøye hvilke oppgaver losen skal ha i broteamet. Losen er kun en rådgiver og har ikke noe formelt ansvar, men som trer inn i broteamet uten noe tilvenning eller opptrening på fartøyet.

Regel – Planlegging og forberedelser
- Personell som har en rolle i broteamet skal gjøre nødvendige kartstudier og personlige forberedelser.

Aktsomhetsnivå

Lav aktsomhet minsker muligheten broteamet har til å oppdage farer og endringer. Dessverre er det ofte mer behagelig å vurdere behovet for aktsomhet lavt på grunn av forventninger om en enkel og rolig seilas enn det er å diskutere og visualisere mulige konsekvenser. Dette gjelder særlig i kjente og enkle farvann.

Lavt aktsomhetsnivå kan også forsinke forståelsen av, og beslutningen om, proaktiv forsterkning av broteamet. Altfor ofte blir det vurdert tilstrekkelig å fortsette med standard bemanning når kompleksiteten gradvis øker.

Spørsmål for å velge aktsomhetsnivå:
- Hva krever denne rollen av meg?
- Hva krever dette oppdraget av meg?
- Enkelt eller vanskelig?
- Hva er vanlig i tilsvarende situasjoner?
- Hvilke roller i teamet må være ekstra aktsom nå?

Regel – Aktsomhetsnivå
- Farene ved å innta for lavt aktsomhetsnivå skal være kjent i broteamet.
- Farvann eller situasjoner med økt vanskelighetsgrad krever økt aktsomhetsnivå.

Situasjonsbevissthet (SA)

Situasjonsbevissthet handler om å være oppmerksom på omgivelsene rundt deg, å forstå hvordan elementer i omgivelsene påvirker dine oppgaver og oppdrag, og å forutse hva som kan skje dersom dette forholdet får fortsette uten din inngripen (Endsley, 1995a).

Figur 3, Situasjonsbevissthet foregår på tre nivåer (alle mentale)

Situasjonsbevissthet foregår mentalt hos hver person i teamet. Evnen til å oppnå og opprettholde SA påvirkes således av personlige tilstander og egenskaper som; forventninger, motivasjon, erfaring, mental og fysisk tilstand, tretthet, individuelle forskjeller, kunnskap, kompetanse, osv. SA påvirkes også av ytre rammer som oppdrag, kontekst, arbeidsplassens utforming, graden av automasjon og organisatoriske betingelser.

Det er viktig å påpeke at Felles SA kun kan oppnås gjennom god kommunikasjon.

Regel – Situasjonsbevissthet (SA)
- Broteamet skal sørge for felles forståelse av oppdrag og sette av tid til å holde alle oppdatert på situasjonsbildet og endringer av prioriteringer.

Teamets sammensetning

Et velfungerende broteam krever at besetningen utfyller hverandre med individuell kunnskap, ferdigheter og holdninger slik at evne til effektiv samhandling opprettholdes til tross for kompleksiteten i det operative miljøet. Oppgaver må utføres under forhold som tidspress, tvetydig informasjon, rask endring og utvikling i scenarier, ressursbehov (belastning), tretthet og mentalt og fysisk stress.

Figur 4, Broteam på KNM Thor Heyerdal (Foto: Petter B. Gulbrandsen / Sjøforsvaret)

Individuell opplæring og utdanning må tilrettelegges, og ressurser må tilføres slik at teamet får trent og operert sammen under alle forhold fartøyet er ment å kunne fungere i. Et godt trent team vil kunne optimalisere fordelingen av ressurser og tilpasse teamets struktur for oppgaven, oppdraget og operasjonsmiljøet.

Regel – Teamets sammensetning
- Teamets sammensetning skal være basert på komplementær kompetanse som sikrer trygg og effektiv navigasjon.

Søvn, tretthet og belastning

Søvnmangel og for høy belastning over tid fører til humørsvingninger, redusert situasjonsbevissthet, problemer med logisk resonnement, konsentrasjon, koordinasjon, hukommelse og svakere motoriske ferdigheter. Mennesker har et gjennomsnittlig behov for 7-8 timers sammenhengende søvn i døgnet (Hirshkowitz, 2005). Militær forskning viser at god søvnkvalitet og fornuftig vaktrotasjon fører til smartere, raskere og mer treffsikre team med økt evne til effektiv utførelse av oppdrag i komplekse militære miljøer (Miller, Matsangas, & Kenney, 2012).

Fem timer sammenhengende søvn minst en gang i døgnet bør være et absolutt minstekrav for å være skikket for en vaktfunksjon ombord, som for eksempel vakthavende navigatør. Det er her viktig å påpeke at fem timer søvn ikke er å anse som en anbefaling da det ikke er tilstrekkelig for normal ytelse i lengden. En tommelfingerregel er at én time søvn gir to timer normal ytelse. 5 timer sammenhengende søvn gir da kun 10 timer ytelse, mens det gjenstår 9 timer av døgnet.

Ved valg av rullering (6/6, 4/8 etc.) er det avgjørende at syklusen går opp i 24 timer. Merk at vaktrotasjon 6/6 ikke gir tilstrekkelig sammenhengende søvn, og at delvis søvnmangel er uunngåelig i denne modellen. 4/8 skift er vist å gi bedre søvnkvalitet enn 6/6 (Short MA, 2015).

Negative effekter av søvnmangel og belastning må begrenses gjennom en kontinuerlig avveining mellom operative krav og personellets fysiologiske behov.

Regel – Søvn, tretthet og belastning
- Fartøyets ledelse skal opprettholde en fornuftig søvn-våkenhetssyklus med et tilpasset rulleringssystem i forhold til oppdragets art og kroppens naturlige 24-timers syklus.

Trivsel og miljø

Trivsel øker teamets ytelse. Et godt miljø kjennetegnes ved at besetningen viser interesse og motivasjon for interne prosesser, samt at de deltar aktivt for å utføre oppgaver individuelt og kollektivt. Videre er gjensidig tillit og respekt viktige forutsetninger for motivasjon og eierskap til fellesskapet. Et klima der tilbakemeldinger er fritt tilbudt og akseptert uten frykt for represalier vil oppleves som inkluderende og øke interessen for teamets oppgaver og mål. Tilpasningsevne til andre teammedlemmer innebærer å vise hensyn og respekt for andre, og en villighet til å lytte til deres meninger.
Stikkord: «Happy ship»

Regel – Trivsel og miljø
- Fartøyets ledelse skal legge til rette for gode samarbeidsmiljøer på bro, og hvert medlem i broteamet skal utvise gode holdninger og støttende adferd for etterlevelse.

Referanser

Cannon-Bowers, J. A., & Salas, E. (1998). *Making Decisions Under Stress.* Washington DC, USA: American Psychological Association.

Endsley, M. (1995a). Toward a theory of situation awareness in dynamic systems. *Human Factors, 37,* 32-64.

Flin, R., O'Connor, P., & Crichton, M. (2008). *Safety at the sharp end: A guide to non-technical skills*. Surrey: Ashgate Publishing.

Hirshkowitz, M. e. (2005). National Sleep Foundation's sleep time duration recommendations: methodology and results summary. *Sleep Health: Journal of the National Sleep Foundation, 1*(1), 40-43.

Miller, N. L., Matsangas, P., & Kenney, A. (2012). The Role of Sleep in the Military: Implications for Training and Operational Effectiveness. In J. Laurence, & M. D. Matthews (Eds.), *The Oxford Handbook of Military Psychology* (pp. 262-281). New York, USA: Oxford University Press.

Orasanu, J. (1995). Training for Aviation Decision Making: The Naturalistic Decision Making Perspective. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 39*(20), 1258-62.

Salas, E., Sims, D. E., & Burke, S. C. (2005). Is there a "Big Five" in teamwork? *Small group research, 36*, 555-599.

Serfaty, D., Entin, E. E., & Johnston, J. H. (1998). Team Coordination Training. In J. A. Cannon-Bowers, & E. Salas, *Making decisions under stress* (pp. 221-245). Washington, DC: American Psychological Association.

Short MA, A. A. (2015). A systematic review of the sleep, sleepiness, and performance implications of limited wake shift work schedules. *Scandinavian Journal of Work, Environment and Health, 41*(5), 425-440.

Sjøforsvarets Navigasjonskompetansesenter. (2018). *Reglement for utøvelsen av militær navigasjon på Forsvarets fartøyer.* Sjøforsvaret. Bergen: Sjef Sjøforsvaret.

Wilson, K. A., Salas, E., Priest, H. A., & Andrews, D. (2007). Errors in the Heat of Battle: Taking a closer look at Shared Cognition Breakdowns Through Framework. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 49*(243), 243-256.

Bruken av CRM i oppøving på Sjøforsvarets fartøyer

Anders Fiskerstrand og Frode Voll Mjelde

Sammendrag

Ved oppøving av Sjøforsvarets fartøyer iverksettes det øvelser og oppdrag som tester besetningene i realistiske operasjoner under krevende omstendigheter. I slike sammenhenger er det viktig at besetningen fungerer som et helhetlig team, og at alle sub-teamene jobber mot felles måloppnåelse. Kan økt bevisstgjøring av CRM-adferd gi positiv effekt på resultatet i oppøvingen?

Bakgrunn for CRM

27.mars 1977 skjedde det en alvorlig flyulykke på Tenerife med to Boeing 747 som kolliderte på rullebanen, og som krevde 583 menneskeliv. I forbindelse med etterforskningen av denne ulykken fant man en rekke faktorer som tydelig viste nødvendigheten av faste rutiner og prosedyrer for trening av teamene i cockpit innenfor situasjonsbevissthet, samhandling og kommunikasjon. CRM kurs og CRM trening ble med dette obligatorisk i luftfart for opprettholdelse av sertifikater.

Senere har dette også funnet veien til den maritime næringen, samt en rekke andre yrker hvor god CRM adferd er kritisk for sikkerhet og effektivitet. For den maritime næringen sin del kom dette inn for fullt på begynnelsen av 1990 tallet, og har i dag blitt et obligatorisk krav fra IMO[1] for dekks- og maskinoffiserer gjennom STCW 2010 konvensjonen. Som et resultat av forskriften og andre internasjonale anbefalinger har samtlige kadetter ved Sjøkrigsskolen, uansett bransje, vært trent i CRM adferd siden 2002. En utfordring med å tilføre slik trening i en skolesituasjon er at kunnskapen ikke nødvendigvis opprettholdes for å gi positiv påvirkning på teamene når de kommer om bord. En løsning kan være å gi fartøyene spesifikke CRM-pakker i forbindelse med oppøving av et fartøy.

Fregatt re-klarering vinteren 2017-2018, fokus på Broteamet

KNM Roald Amundsen skulle i november 2017 klareres iht normale oppøvingssykluser. Besetningen opplevde en del store utskiftninger etter endt oppdrag i SNMG våren 2017, samt at avvikling av ferie og avspasering etter samme oppdrag medførte mye stilleligge ved Haakonsvern på ettersommeren og høsten. Med disse utfordringen møtte besetningen til klarering med stort fokus på å løse oppdraget, men med varierende erfaringsnivå. Det nye Broteamet fremstod med tydelige utfordringer på samhandling innen eget team og mellom teamene de koordinerte oppgaver med.

Klareringen resulterte dessverre i at fartøyet ikke bestod klareringen, og måtte prøve på nytt like etter årsskiftet. Det var lite tid trening og øving mellom klareringene, og besetningen hadde svært begrensete muligheter til å tilføre ny kunnskap før re-klarering. Observasjoner gjort på broteamet under første klarering

[1] *IMO – International Maritime Organization*

Figur 1, Input-process-output modell for CRM trening KNM Roald Amundsen

tydet på at systemforståelse og individuell kompetanse stort sett var tilfredsstillende, slik at de største utfordringene dermed lå på selve samhandlingen i teamet; mer spesifikt på rolleforståelse, kommunikasjon og felles mentale modeller. Oppdaterte felles mentale modeller er viktig for å skape forståelse for oppdraget, samtidig som det fører til økt interesse og motivasjon i teamet for sine oppgaver (Salas, Sims, & Burke, 2005). Etter en avveining mellom tid til rådighet og treningsbehov ble det bestemt at broteamet skulle delta på en skreddersydd 4-timers pakke med CRM Instruktører på Navkomp. Det ble benyttet en input-process-output modell hvor (1) input; baserte seg på rapporten fra klareringen, krav til ytelse og samtaler med involvert personell, (2) process; tilpassing av CRM teori for besetningens identifiserte behov, og (3) kompetanseheving av prinsipper for samhandling frem mot reklarering (fig 1).

Input

Rapporten fra klareringen viste at Navigatør og assistent evnet å bygge godt bilde mellom seg og Surface ops. Med kontroll på hver sin radar (3cm og 10cm) verifiserte de kontakter med utkikker og Surface ops som skapte god kontroll på andre fartøy i området. De viste med dette gode innarbeidete roller i forbindelse med vanlig seilas, trolig en effekt av at de har hatt kontinuerlig trening i disse funksjonene hver gang de gjennomfører seilas. De samme rolleinnehaverne viste også meget god innlevelse og motivert adferd under klareringen. På den måten oppnådde de en intern aksept for ytre påkjenninger og komplekse omgivelser, noe som igjen medførte trygg og sikker navigasjon, selv i en stresset situasjon. Dette forholdet ble belyst i undervisningen som et eksempel på positiv CRM adferd hvor drill, kommunikasjon og aksept av situasjonens kompleksitet kan føre til høy ytelse under vanskelige forhold.

Imidlertid kan dette samarbeidet bare ses på som et lite sub-team i det store teamet som settes opp under «klart skip» på en fregatt. Sub-teamet var i dette tilfellet meget velfungerende, mens det store «klart skip» teamet ikke evnet samme ytelse. Broteamet fremstod med tydelig tegn på rolleuklarheter ved flere anledninger. Flere medlemmer i teamet hadde fått nye roller siden forrige oppøving (FOST) og deployering (SNMG), samt at det også var kommet en del nye personer inn i teamet. Rapporten indikerte at enkelte medlemmer i teamet ikke helt klarte å slippe taket i tidligere roller og påtok seg dermed flere oppgaver enn de skulle hatt, et resultat av at den som var satt inn i ens forrige rolle ikke hadde fått nødvendig opplæring eller at det ikke var gjort oppdaterte rolleavklaringer. Ved bortfall av faste medlemmer var det mangel på felles rolleforståelse i teamet hvor ingen overtok rollen til medlemmet som måtte forlate sin plass.

Rapporten beskrev flere tilfeller av utfordringer ved kommunikasjon, hvor personell ikke fikk den informasjonen de trengte for å løse oppdraget på en god måte. I noen tilfeller førte mangelfull kommunikasjon til at teamet mistet felles situasjonsforståelse, noe som igjen reduserte evnen til initiativ proaktiv adferd. Manglende oppdatering av prioriteringer etter hvert som situasjonen utspilte seg svekket teamets situasjonsforståelse, omstillingsevne og koordinering av oppgaver. Det handler om å taske personell mot de rette oppgavene til rett tid, eksempelvis som å informere utkikker og skyttere om retninger og prioriteter når man forventer trusler fra sjøgående eller landbaserte enheter.

Utfordringene i et klart skip broteam er at de normalt sett jobber sammen i mindre team innenfor ulike områder under vanlig seilas, samt at også enkelte av dem ikke har sin normale funksjon på bro. Man har ikke bare en utfordring på at de jobber i ulike team, men man har også spredning i grad og alder fra nye vernepliktige til erfarne offiserer. Dette er klassiske kombinasjoner som gir utfordringer i teamprosessene. Tilbakemeldingen fra klart skip broteamet var varierende ift hvilken bakgrunn den enkelte hadde og i hvilken fase man var i.

Process

Basert på innspill fra rapporten og besetningen selv resulterte dette i fokus på tre hovedmomenter under CRM undervisningen: Rolleavklaring, Eksplisitt koordinering og Kommunikasjon (Figur 2), hvorpå situasjons-

Figur 2, CRM fokus retrening KNM RAMU

bevissthet (SA), Felles mentale modeller (FMM) og støttende adferd i team ble utledet og forklart på bakgrunn av disse tre emnene.

Kommunikasjon er utveksling av informasjon, tilbakemeldinger og respons og er en viktig aktivitet i koordinering mellom teamets medlemmer for å oppnå sine mål. God og riktig kommunikasjon innad i broteamet er en meget viktig faktor for oppgaveforståelse og oppdragsløsning. Elementer som fremmer god kommunikasjon i team kan være: åpenhet, aktiv lytting, tydelig innhold, tydelig fremføring, timing (rett informasjon til rett tid, og i passelig mengde) og felles mentale modeller av teamets oppgaver.

God rolleavklaring øker teamets effektivitet og evne til måloppnåelse. Mangelfull rolleavklaring har vist seg å være en av de vanligste grunnene til teamsvikt, som igjen har vært medvirkende eller direkte årsak til tap og skader av personell og materiell og til mangelfull utførelse av oppdrag (Flin, O'Connor, & Crichton, 2008). Klar og tydelig rolleavklaring er derfor meget viktig både for teamets standard operasjonsmønster og for nye eller spesielle operasjoner.

Eksplisitt koordinering av oppgaver innebærer at teamets leder delegerer oppgaver, samt hvilke prioriteringer som gjelder. Medlemmer av broteamet får dermed en klar og tydelig oppgavefordeling som definerer hvordan de forholder seg til oppdraget. Uttalte prioriteringer øker oppmerksomheten for tildelt oppgave og minsker mulighetene for misforståelser og antakelser (Serfaty, Entin, & Johnston, 1998). Team som evner til å sette av tid til å holde alle oppdatert på prioriteringer og situasjonsbilde øker teamets situasjonsforståelse og evne til måloppnåelse (Orasanu, 1995).
Samtlige fokuspunkter ble belyst i løpet av undervisningen, og besetningen knyttet faktiske hendelser og opplevelser til CRM teorien. CRM-undervisningen på Sjøkrigsskolen fokuserte dermed på besetningens egen opplevelse av positiv og negativ CRM-adferd i den hensikt å øke teamets kunnskap og forståelse for samhandling i operative team. Besetningens gode involvering førte til flere fruktbare diskusjoner i løpet av undervisningen.

Output

I løpet av CRM undervisningen demonstrerte besetningen en økt interesse og kunnskap om gode prinsipper for samhandling, samt en økt forståelse for hvordan god CRM-adferd ville ha positiv effekt på sitt eget teams ytelse. Besetningen uttalte at ved en full oppøving ville et fullt CRM kurs være positivt, men at det i gjeldende setting ikke var tid til dette. Flere av medlemmene i broteamet innehar allerede CRM kurs og trening fra tidligere, men det var en utstrakt enighet i at denne re-treningen på fire timer gav dem den en økt bevisstgjøring for positiv CRM-adferd som var nødvendig for å takle utfordringene med re-klarering.

Ved ny re-klarering gjennomførte broteamet sin «klart-skip» funksjon til karakter Bestått, og var godkjent til kampkraft nivå 2. For å oppnå dette nivået må besetningen ha vært igjennom et fult oppøvingsløp (OPUS) og gjennomført og bestått FOST. Det er også dette nivået de må inneha for å bli sendt ut i internasjonale operasjoner. De fikk i dette forsøket vist kunnskapene og ferdighetene sine på en mye bedre måte blant annet som følge av en mye bedre samhandling i teamet og mer fokus på felles mentale modeller. Det som her er viktig å bemerke er at de mellom disse to forsøkene fikk minimalt med tid til trening (2,5 dager i sjøen) og heller ikke fikk tid til noe annen undervisning enn den halve dagen med CRM fokus. Det er derfor betimelig å stille seg spørsmål om graden av betydning CRM kurset faktisk har i et oppøvingsøyemed.

Drøfting

Et tilpasset fire timers CRM kurs var den eneste treningen som ble gjennomført for et felles broteam mellom disse to klareringene, noe som kan tyde på at det hadde stor betydning for forskjellen på teamets ytelse mellom første og siste klarering. En interessant observasjon er at fregattvåpenet ikke vurderer CRM-adferd og teamtrening som tilstrekkelig relevant i faser med lite tid tilgjengelig. Fokuset havner gjerne på mer konkrete oppgaver som tabletop-øvelser innenfor krigføring eller trening på brann og havari. Det kan være vanskelig å velge det ene eller det andre med begrenset tilgang på tid og ressurser. En kombinasjonsmodell hvor CRM trening blir en integrert del av trening på tekniske ferdigheter kan øke robuste team-prestasjoner under stress og i høy risiko.

I første forsøk på klarering ble det også kommentert fra teamet selv at det var et fåtall igjen av dem som hadde deltatt på fartøyets fulle oppøvingssyklus via OPUS løpet og FOST, og således manglet både ferdigheter og samhandling i teamet. Det sier seg da selv at det er en rekke personer som har kommet inn i det nye teamet uten nødvendigvis å helt ha funnet sin rolle og posisjon. Det er ikke alle roller som er like tydelig definerte og som gir klare føringer for hva man kan og skal si fra om. På en bro med 10-12 personer direkte involvert inne på bro og ytterligere 4-8 personer ute på dekk så vil det fort bli usikre kommunikasjonslinjer og kommandoforhold dersom dette ikke er klargjort på forhånd og at alle er innforstått med sin viktige plass i det store bildet. Et eksempel på forståelse og trygghet i tildelt rolle fra siste klarering var da utkikken korrigerte info som taktisk vaktsjef gav ut på bro, fordi han har fått med seg viktig info fra PA eller annet samband. Gode team prosesser førte frem til at utkikken faktisk turde å si fra og korrigere feil SA hos taktisk vaktsjef slik at man sammen presterte på et høyere nivå. Her handler det ikke bare om roller og team men også om felles mentale modeller og situasjonsbevissthet. Det er ikke slik at alle kan få med seg alt til enhver tid - og gode team hjelper hverandre med å samle inn og prosessere viktig informasjon.

På tilsvarende måte gjennomførte Hurtigruten et forsøk i samarbeid med navkomp for 43 av sine navigatører gjennom en 4 ukers periode. Her ble navigasjonsteamene bestående av kaptein, overstyrmann, 1. styrmann og sikkerhetsoffiser sendt i land for deltakelse på et 4-timers CRM kurs ifm kailigge i Bergen. Her blir de påført et ekstra element ifm den korte tiden de har i Bergen som snuhavn. I disse timene fikk de en CRM introduksjon med teori og praktiske caser tilpasset Hurtigrutens operasjoner, hvor et av fokusområdene handlet om å etablere evnen til «å si fra» til teamet. Tilbakemelding etter kurset viste en utelukkende positiv holdning til bruken av CRM, og resultatet fra teamenes operative tjeneste på Hurtigruten viste en signifikant positiv effekt på hvordan de i ettertid fungerte som team på bro (Espevik, Rose Saus, & Kjellvold Olsen, 2017).

CRM som fast del av oppøving

Basert på de erfaringene som er gjort i forbindelse med re-klarering av KNM Roald Amundsen og forsøket med 43 navigatører fra Hurtigruten ser man helt klart potensiale for at CRM fokus tilfører økt yteevnen og prestasjonen til ulike team. Det er alltid en utfordring å putte inn nye elementer i en allerede presset oppøving, men klarer man å oppnå den ønskede effekten som fremkom i disse to tilfellene vil innføringen av CRM i oppøving kunne være med på å effektivisere og bedre resultatet. Anbefalingen er at fartøy i Sjøforsvaret øker fokus på CRM i den hensikt å bedre sikkerheten under seilas, å gi økt utbytte av oppøving og å forsterke operativ yteevne.

Referanser

- Espevik, R., Rose Saus, E., & Kjellvold Olsen, O. (2017). Exploring the core of crew resource management course: speak up or stay silent. *International Maritime Health, 68*(2), 126–132.
- Flin, R., O'Connor, P., & Crichton, M. (2008). *Safety at the sharp end: A guide to non-technical skills.* Surrey: Ashgate Publishing.
- Orasanu, J. (1995). Training for Aviation Decision Making: The Naturalistic Decision Making Perspective. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 39*(20), 1258-62.
- Salas, E., Sims, D. E., & Burke, S. C. (2005). Is there a "Big Five" in teamwork? *Small group research, 36,* 555-599.
- Serfaty, D., Entin, E. E., & Johnston, J. H. (1998). Team Coordination Training. I J. A. Cannon-Bowers, & E. Salas, *Making decisions under stress* (ss. 221-245). Washington, DC: American Psychological Association.

Maritim kriseledelse i nordområdene og lederkompetanse - erfaringer fra marpart-prosjektene

Natalia Andreassen, Odd Jarl Borch, Petter Lunde og Frode Voll Mjelde

Sammendrag

Den betydelige endringen i aktivitetsmønsteret i nordområdene har skapt et behov for økt fokus på maritim beredskap og samvirke over landegrensene i nord. MARPART-prosjektene har sett nærmere på beredskapsutfordringer og beredskapsorganisering for nordområdene. I den forbindelse har det i de siste årene vært et utstrakt sivilt-offentlig samarbeid i de arktiske landene rettet mot maritim beredskap i denne regionen. Denne teksten beskriver prosjektets formål og erfaringene så langt.

MARPART illustrasjonsfoto (kilde: NORD Universitetet)

Fagnettverk for studie av maritim beredskap

De siste fire årene har det vært et utstrakt samarbeid mellom fagmiljø i de arktiske landene rettet mot maritim beredskap. De såkalte MARPART-prosjektene har sett nærmere på beredskapsutfordringer og beredskapsorganisering i Norge og våre naboland; Grønland, Island, Sverige og Danmark (MARPART, 2018). Målgruppen er akademia, myndigheter, private bedrifter og sivilt samfunn som er involvert i eller har ansvar for den maritime beredskapen i nordområdene. Sikkerhet og beredskap i nord har en rekke utfordringer knyttet til klima, vær, et sårbart økosystem og en begrenset infrastruktur. Både kommersielle aktører og regjeringer understreker viktigheten av å øke beredskapen for å forberede seg på uønskede hendelser (Utenriksdepartementet, 2011).

Et stort antall forskningsmiljø har gått sammen i MARPART-prosjektene som har vært ledet av Nordområdesenteret ved Handelshøgskolen, Nord universitet. Prosjektet finansieres gjennom Arktis 2030 programmet i Utenriksdepartementet, Nordland fylkeskommune og ti institusjoner i Norge, Russland, Grønland, Danmark og Sverige. De norske fagmiljøene omfatter Sjøkrigsskolen, Politihøgskolen, Norges Brannskole, Universitetssenteret på Svalbard, Institutt for forsvarsstudier, Forsvarets Forskningsinstitutt, UiT og Nord universitet.

Endring i aktivitetsmønsteret krever nytt fokus på kompetansemønsteret

Norge har den største aktiviteten i Arktis. Større trålere opererer helt opp mot 83 grader nord for Svalbard på jakt etter reke og torsk. Det bygges i 2018 nærmere 30 nye ekspedisjonscruisebåter som skal operere i Arktis og Antarktis. Økt gjennomgangstrafikk med farlig last og økt militær trafikk representerer andre usikkerhetsmoment. Med endring i aktivitetsmønsteret i nordområdene blir det også et behov for fokus på maritim beredskap, samvirke over landegrensene i nord, og kompetanseoverføring. For fagmiljøene er det viktig å få til en erfaringsutveksling som kan lede til en mer effektiv utdanning av nøkkelpersonell i de nasjonale beredskapssystemene så vel som i de virksomheter som skal operere i regionen (Norges offentlige utredninger, 2016).

Samvirke er et nøkkelord for beredskapsutdanningen når en snakker om aksjoner som kanskje omfatter et cruiseskip med flere tusen passasjerer, eller et tankskiphavari. Store avstander og begrensede ressurser gjør at alle må delta. Da et norsk kystvaktskip mistet et av mannskapene over bord for en stund siden var over 20 fartøy med i letingen. Majoriteten av disse var russiske. De lokale forholdene krever samarbeid over organisasjons- og landegrensene, men også internt mellom avdelinger og nivå. Kombinerte operasjoner som for eksempel pågående livstruende vold og grenseoverskridende innsats er særlig krevende kompetansemessig. Det er behov for å se på hele kompetanseverdikjeden fra utdanningsprogrammer og kurs, til trenings- og øvingsopplegg.

Samvirke over etats- og landegrenser

I Marpart-konsortiet har en sett på beredskapsressurser i flere land i Arktis, og utfordringer ved forskjeller i organisasjon, ledelse, planverk og beslutningsstøtteverktøy i beredskapsorganisasjoner. Noe av utfordringene er knyttet til manglende forståelse for ledelsesrollene, spesielt ved store hendelser. Beredskapssystemet innebærer en rekke aktører i et tett samspill, fra kaptein og offiserer om bord i havaristen, skadestedsledere på sjø, redningsledere og aksjonsledelse på landsiden, til politi, brannetat, helse og olje- og strålevern. Denne mosaikken av spillere krever betydelig innsats innen koordinering, kommunikasjon og kontroll, og forståelse for hverandres ansvarsområder. Her har forskerne i MARPART-prosjektene samlet inn erfaringer gjort i reelle hendelser og øvelser der samvirke har stått i fokus.

Sammensatte operasjoner og krav til kompetanse

I store hendelser som for eksempel alvorlige branner eller masseevakuering kan forskjeller i institusjonelle rammeverk, operasjonelle krav, vurderinger av risiko og kapasitet, aksjonsmønstre og kommandosystemer skape både forsinkelser og en mindre effektiv aksjon. Kompleksiteten og volatiliteten i nordområdene påvirker oppsett av kommando- og koordineringssystemer og relevansen av forhåndsdefinerte prosedyrer. Dette krever evne til improvisasjon både hva angår ressursbruk og valg av løsninger. Det kreves bedre kunnskap i samordning og dynamiske evner for å klare rask omorganisering av tilgjengelige og egnede ressurser.

Ved den nyetablerte NORDLAB ved Nord universitet i Bodø er det bygd opp en skreddersydd simulator-styrt trenings-, og testarena der en skal øve koordinering, kommunikasjon og kontroll over institusjonsgrenser, med særskilt fokus på nordområdene. Trening og øving med bruk av simulatorer kombineres med fullskalaøvelsen Øvelse Nord der alle nødetater, sivile og militære ressurser og studenter øver sammen.

Læring av Sjøkrigsskolens erfaringer

Sjøkrigsskolen har jobbet med utdanning for den norske marinen i veldig mange år. Det er mange elementer i læringspraksis som har vært brakt inn knyttet blant annet til forståelse av arktiske forhold, lovverket og overgang til stabsledelse ved hendelse. Ressursstyring, ressurstilgang og kommunikasjon øves i komplekse scenarier (Mjelde, Lunde, Bolstad, & Gloppen, 2017). Menneskelig faktor og ikke minst evne til å jobbe i team har et spesielt fokus for beredskapstrening i Sjøforsvaret. Det som går igjen i internasjonalt erfaringsmateriale når teamsvikt får store konsekvenser er mangelfull eller dårlig rolleavklaring og integrasjonsevne (Flin, O'Connor, & Crichton, 2008). God rolleavklaring, god kommunikasjon og god koordinering er derfor fremhevet som tre kritiske ledelseskompetanse-elementer. Ved Sjøkrigsskolen har en god erfaring med kombinasjon av ulike øvelsesformer, inklusiv bruk av både virtuelle (simulator) og reelle enheter og treningsmiljøer.

Øvingskonsepter utvikling og simulering

En bedre plattform for beslutningstaking kan opprettes gjennom grenseoverskridende samarbeid om grunnopplæring, spesialiserte kurs, seminarer, øvelser, samt å være involvert i debriefing og dokumentasjon, evaluering og formidling knyttet til øvelser og hendelser. I MARPART-prosjektene arbeides det nå med utvikling av utdanningskonsepter og scenarier for ulike lederroller i maritim beredskap. Nært samspill og dialog og flernasjonale opplæringsordninger som inkluderer både universiteter og profesjonshøgskolene kan gi bedre forståelse av institusjoner, lederroller og nivå, og planverk i andre institusjoner. Polarkodekurs for sjøfolk i arktis kan blant annet være et startpunkt for tettere samarbeid.

Integrasjon av simulatorsentre mellom universitetene vil kunne gi en skreddersydd undervisningsinfrastruktur der en utnytter de ulike fagmiljøenes spisskompetanse.

Det er derfor behov for felles utvikling og uttesting av øvingskonsepter. Dette tas nå videre fra MARPART-prosjektene i et stadig voksende fagnettverk under UArctic-paraplyen for sikkerhet og beredskap med rundt 25 universitet og forskningsinstitutt (The University of the Arctic, 2018).

Referanser

Flin, R., O'Connor, P., & Crichton, M. (2008). *Safety at the sharp end: A guide to non-technical skills.* Surrey: Ashgate Publishing.

Justis- og beredskapsdepartementet. (2014, November 24). *Mål for justis- og beredskapssektoren.* Retrieved Mars 2017, from Regjeringen.no: https://www.regjeringen.no/no/tema/lov-og-rett/innsikt/mal-for-justis--og-beredskapssektoren/id2076236/

MARPART. (2018, June 22). *www.marpart.no.* Retrieved from Maritime Preparedness and International Partnership in the High North (MARPART): https://www.nord.no/no/om-oss/fakulteter-og-avdelinger/handelshogskolen/senter/nordomradesenteret/Sider/MARPART.aspx

Mjelde, F. V., Lunde, P., Bolstad, M., & Gloppen, H. (2017). Nasjonal virtuell beredskap. *Necesse, 2*(1), p. 68.

Norges offentlige utredninger. (2016). *NOU 2016:19 Samhandling for sikkerhet.* Forsvarsdepartementet. Oslo: Departementenes sikkerhets- og serviceorganisasjon Informasjonsforvaltning.

The University of the Arctic. (2018, June 22). Retrieved from UArctic: https://www.uarctic.org

Utenriksdepartementet. (2011). *Nordområdene - Visjon og virkemidler.* Stortingsmelding nr. 7, Oslo.

DEL 2

Militær praktisk navigasjon

Innføring av Seilashåndbok for Operativ Marine

Vibeke Thuesen

Sammendrag

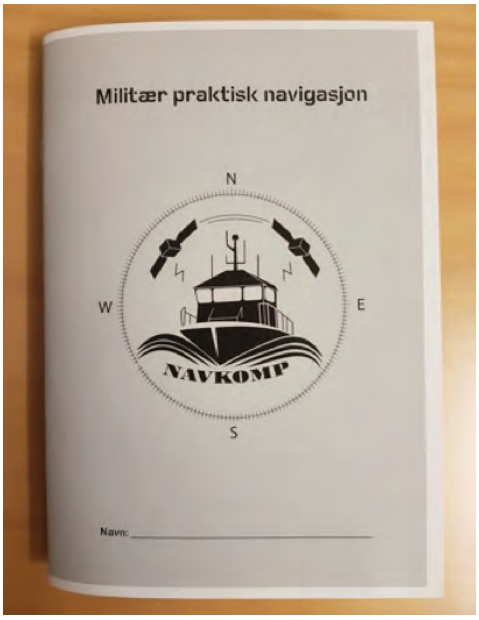
Seilasboken er utviklet til bruk i faget Militær Praktisk Navigasjon for Operativ Marine på Sjøkrigsskolen. Den er ment å være et verktøy som kan hjelpe eleven med å effektivisere refleksjonsprosessen for å fremme utvikling og læring. Boken er for tiden under utprøving i OM2, og skal medbringes på alle seilaser og øvinger. Denne artikkelen beskriver idéen bak boken og erfaringer så langt.

Prosessering og refleksjon i etterkant av en hendelse er en essensiell del av læring. Noen ting må man tenke mer igjennom før bitene faller på plass og man virkelig forstår. Men det føles ikke alltid så viktig å ta seg tid til denne delen, å tenke igjennom, når neste hendelse og neste ting man skal gjøre i hverdagen venter rett rundt hjørnet. *Hvilket verktøy kan hjelpe en person, i en hektisk hverdag, til å reflektere bedre over egne avgjørelser og prestasjoner i etterkant?* Hvor nytteverdien er høy, sammenlignet med tiden man bruker på det. Dette, blant annet, var tanker bak utviklingen av Seilasboken til bruk i faget Militær Praktisk Navigasjon for Operativ Marine på Sjøkrigsskolen. (Figur 1).

Bakgrunn

Ideen om boken startet i januar i år, den ble tatt i bruk av OM2 på deres første kveldsseilas i februar dette semesteret. Vi besluttet oss for å starte bruken av boken med den hensikt å utvikle den etter hvert, dersom det viste seg å være noe som fungerte for kadettene. (*Vi* er da Bjarne Haukås (Faglærer MPN) og meg selv (Instruktør MPN)). Seilasboken har vært i bruk i snart et semester for OM 2 klassen på Operativ Marine.

Som nevnt var det å effektivisere refleksjonsprosessen for økt læring motivasjonen for å utvikle boken. Hvert semester i faget Militær Praktisk Navigasjon har



Figur 1, Seilasbok i Militær Praktisk Navigasjon. Boken er tilpasset størrelsen på US uniformens sidelomme. Hensikten er at den skal være enkel å ta med seg for bruk på kveldsseilaser og helgeseilaser.

kadettene på Operativ Marine tre kveldsseilaser, en helgeseilas og syv simulatorøvinger hver. De får utlevert en øvingsordre før hver seilas som blant annet beskriver mål og fokusområder for seilasen. Skipsførere og veiledere på Navkomp følger opp kadetten underveis i seilasen, og kommer med påfølgende tilbakemelding etter endt seilas. Det holdes videre en felles debrief etter at alle elevene har gjennomført. Det har blitt observert at kadettene i varierende grad noterer ned tilbakemeldinger etter seilas sin, noen skriver flittig mens andre velger å ha en dialog uten å notere. Jeg husker selv jeg forsøkte å notere ned det skipsførerne og veilederne ga tilbakemeldinger på, og noen av dem kunne være så ivrig at jeg egentlig burde hatt med meg båndopptaker. Mens andre hadde en mer kortfattet måte å gi tilbakemeldingen på. Jeg husker jeg synes det noen ganger var frustrerende at de ikke kunne være mer samkjørte i forhold til hva de la vekt på. Men så, hva gjorde jeg med tilbakemeldingene? Hva gjør kadettene med dem i dag? *Forstår* man bakgrunnen for tilbakemeldingen, og er noe *gjenkjennbart*? Hvis ikke blir den jo lett forkastet, og mye læring kan gå tapt. *Hva synes man selv om seilasen sin? Og hvor mye tid skal man bruke på dette?*

Figur 2, Navigatørens notater

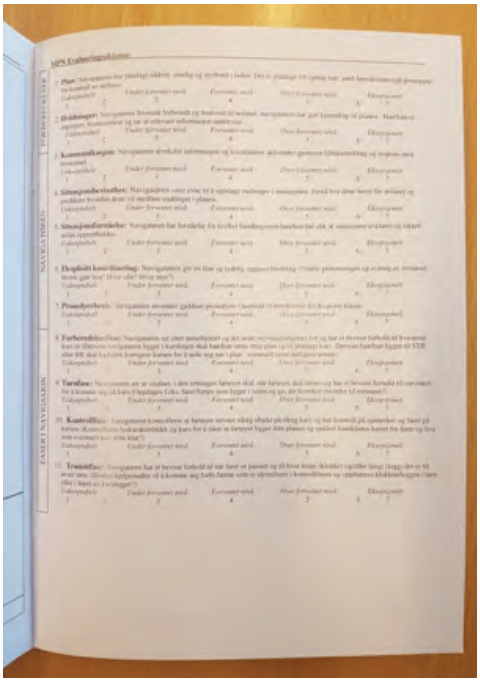
Innholdet

Tanken er at Seilasboken skal gi kadettene mulighet til å samle alle tilbakemeldingene de får etter endt seilas på ett sted. Utformingen er ment å hjelpe kadetten til å få ut essensen i tilbakemeldingen, samt fremtvinge egenrefleksjon. «Refleksjonsmodulen» i boken inneholder to sider for hver seilas med dato, øvelse og mål. Den ene siden inneholder *navigatørens notater*, hvor kadetten kan notere som ønskelig, samt *fokusområder til neste seilas.* (figur 2).

Under fokusområder er det tiltenkt at skipsfører/veileder skal trekke ut maksimalt tre punkter fra tilbakemeldingen sin, som de mener kadetten skal fokusere på ved neste seilas, og signere. Tanken er at det da skal bli lettere å følge opp tilbakemeldingen. Den kan enkelt tas frem og gjennomgås i etterkant. Kadetten kan også ta frem boken før neste seilas og minne seg særskilt på de tre fokusområdene, samt se over andre notater som eventuelt ble gjort.

På neste side er det et *evalueringsskjema* (figur 3) med 11 påstander hvor hensikten er at eleven selv, ut i fra egne notater og tilbakemeldinger fra veileder, skal krysse av for hvordan han/hun presterte på en skala fra 1-5.

Vi hadde en del tanker rundt evalueringsskjemaet. Burde vi ha ved en forklaring til det? Burde veilederne fylle det ut og ikke eleven? Ville det være effektivt nok til å fungere etter hensikt? Hensikten vår var således egenrefleksjon og ikke at det skulle være «korrekt» utfylt. Hvis skjemaet kunne få eleven til å tenke gjennom seilasen sin var egentlig hensikten med det



Figur 3, Evalueringsskjema

nådd. Vi la ikke noe krav til at skjemaet skulle fylles ut, kadetten kunne benytte seg av det hvis det fremstod som formålstjenlig for den enkelte.

Et annet ønske vi hadde med utviklingen av Seilasboken var å få samlet de viktigste verktøy og prinsipper kadetten kan bruke til en seilas, på ett sted. Dette være seg «Faser i optisk navigasjon», «Faser i radar navigasjon», «Distanse og fartstabell», «Prosedyrer», «Notasjoner» etc. (NAVKOMP, 2018). Vi ba elevene i OM2 om innspill til hva de kunne tenke seg å få samlet i en slik bok. De kom med flere ideer, blant annet til forskjellige sjekklister til bruk ombord på skolefartøyene; klargjøring til avgang, klargjøring til ankomst, overlevering navigatør etc. som er lagt til i boken.

Erfaringer så langt – etter 4 mnd

I starten, før boken ble laget hadde vi god dialog med elevene i OM2 som nå prøver ut boken. Vi hadde videre en «klassens time» med elevene i mai for å høre hvordan de opplevde den. Hovedinntrykket vårt var at de likte godt å ha viktig navigasjonsmessig informasjon samlet på ett sted, samt å ha én plass for å samle tilbakemeldinger. Oppfatningene om nytteverdien av skjemaet var delte, og det ble forslått og heller utforme spørsmål enn å formulere det som påstander. Det ble også foreslått at veilederne skulle fylle det ut i stedet for kadetten. Videre ble det diskutert om det var mulig å lage plass i boken til å skrive ned notater fra felles debrief etter endt seilas. Beskrivelse av Sjøveisregler var også ønskelig. Hovedinntrykket fra møtet var at enkelte brukte boken veldig aktivt mens andre brukte den i mindre grad. Elevene virket interessert i å videreutvikle Seilasboken.

Vi diskuterte i forkant av bokens utgivelse om skipsfører/veileder skulle fylle ut evalueringsskjemaet i stedet for kadetten selv. Det som taler for dette er at det kan være vanskelig å bedømme sin egen seilas, hva har man fått med seg etter å ha «kokt i navigatørstolen?» Det som taler mot dette er at det overlates til veileder å bedømme kadettens seilas, noe som ikke nødvendigvis inkluderer kadetten selv i prosessen. Kadetten kan således «unnlate å forstå, men bare høre etter», og dermed miste verdifull egenrefleksjon. Det husker jeg selv at jeg kunne finne på å gjøre, noen ganger er det godt å bare høre etter(..)Skjemaet kan også begynne å bety så mye mer enn hva hensikten med det er, seilasene kan oppleves som «eksamens» seilas. *Uavhengig av skjemaet skal skipsfører/veileder fortsatt gi sin tilbakemelding til kadetten som tidligere.*

Hvis skjemaet får eleven til å tenke over seilasen sin er egentlig hensikten med det nådd. Men vi tar all tilbakemelding til etterretning, og spesielt når den kommer fra brukerne av boken.

Som nevnt gikk det kort tid fra ideen oppstod til boken var i bruk. Vi trenger tid til å samle erfaringer for å gjøre den best mulig. Vi opplever at kadettene er interessert i å utvikle boken, og det tar vi som et positivt tegn på at Seilasboken kan utgjøre en forskjell for læring. Kanskje den på sikt også kan bli elektronisk, en app.

Navkomp og elevene fra OM2 2016-2019, samt Nils Eivind Skaar (Nav.off KNM Roald Amundsen) som hjalp oss å utvikle Seilasboken, ønsker at den i fremtiden skal kunne fungere for flest mulig etter hensikten; å være et verktøy som kan hjelpe eleven med å effektivisere refleksjonsprosessen, for å fremme utvikling og læring. Man lærer best det man innser selv.

Referanser

Haukås, B., Thuesen, V., & Skaar, N. (2018). *Seilashåndboken*. Bergen: Navkomp.

NAVKOMP. (2018). *SNP 500, Reglement for utøvelsen av militær navigasjon på Forsvarets fartøyer.* Sjøforsvaret. Bergen: Sjef Sjøforsvaret.

Bevisste innstillinger på instrumenter for å bidra til økt situasjonsbevissthet i navigasjon

Bjarne Haukås

Sammendrag

Bakgrunnen for at jeg ønsker å skrive denne artikkelen er basert på erfaringer fra mønstringer, egenbaserte erfaringer og en hendelse som ble opplevd nord av Fleslandskjæret lykt, utenfor Bergen, høsten 2016. Hovedbudskapet er å være bevisst på innstillingene vi benytter på teknisk utstyr, slik at de tjener til hensikten, slik at vi kan unngå ulykker.

Det rapporteres generelt for få navigasjonshendelser i Sjøforsvaret i dag i forhold til det antall hendelser som faktisk eksisterer, noe som gjør det vanskelig for Sjøforsvaret å bli en lærende organisasjon. Med bakgrunn i dette ønsker jeg å bruke en hendelse, som kunne tatt livet av en mann på vannscooter, som bakteppe for å illustrere viktigheten av å ha bevisste innstillinger på det utstyret vi benytter i våre beslutningsprosesser. Jeg tar for meg radaren som er navigatørens viktigste hjelpemiddel i mørket for å illustrere poenget.

Hendelsen

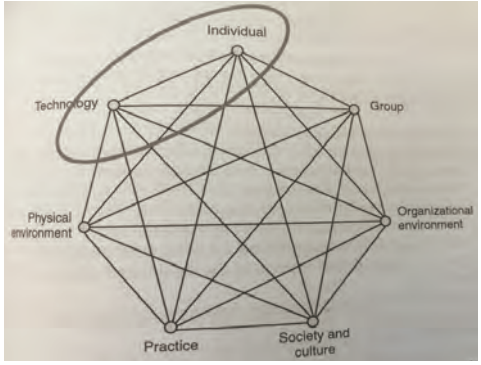
Undertegnede la en høstkveld i oktober 2016 ut på kveldsseilas med en Operativ Marine klasse fra Sjøkrigsskolen. For at elevene skulle få et hensiktsmessig område å trene i og for at vi skulle holde oss innenfor tid og rom begrensningene, skulle jeg navigere fra Haakonsvern til Austevoll og fra Austevoll og tilbake til Haakonsvern. Perioden i mellom navigerte elevene med undertegnede som veileder. På vei sydover var det lyst og alle hjelpemidler i terrenget var dermed synlige; det var kun behov for kikkert for detaljorientering og radaren var på og tilgjengelig ved behov. På returen var det mørkt og jeg hadde «ingen» sikkerhetskontrollør. Jeg benyttet meg likevel av en elev som jeg hadde fått inntrykk av å ha de rette holdningene i tillegg til å være årvåken. Vedkommende ble satt i min vante posisjon. Jeg tunet så radaren for ham slik jeg mente bildet burde være og ba ham rapportere ekko forenfor tvers på vei nordover. Jeg observerte at han gjorde dette i tillegg til at jeg hadde et blikk i min egen radar. Men mitt hovedfokus var "optisk kontroll", og å se ut og aktivt benytte kikkert i det vi dundret nordover i 36 knop. Ved passering Fleslandskjæret lykt rapporterte eleven et ekko forut. Jeg så i kikkert men så ikke noe og reduserte farten og så i kikkert igjen da jeg så en skygge og umiddelbart ga rorordren styrbord tjue. Etter en kort stund passerte en skygge, med et svært svakt lys på babord side av fartøyet. Farten ble redusert ytterligere og fartøyet ble turnet rundt for å se hva dette var. Da vi kom ned til objektet viste det seg at objektet var en forkommen kar på en vannscooter med motorhavari. Det svake lyset vi hadde registrert var fra en lighter som føreren holdt opp i mangel på andre lysremedier. Hendelsen var en nærdøden ulykke som alle på sjøen ønsker å unngå. Min påstand er at navigatørkorpset ikke er bevisst nok på utnyttelsen av det utstyret vi har tilgjengelig.

Den sosiotekniske systemmodellen

Hendelsen beskriver et eksempel som beviser at det er svært viktig at navigatører benytter alle tilgjengelige hjelpemidler og utnytter organisasjonen for å danne seg

et best mulig situasjonsbilde. Men har vi egentlig et bevisst forhold til bruken av tilgjengelige hjelpemidler? Og ikke minst; er innstillingene på slikt utstyr hensiktsmessig og hjelper disse innstillingene oss med å skaffe oss et bedre situasjonsbilde? Tjener utstyret hensikten? Jeg skal ta for meg radar som er det viktigste hjelpemidlet navigatører kan benytte seg av i mørket, men den gir også verdifull informasjon i dagslys. Hovedhensikten med et slikt hjelpemiddel er å bidra med informasjon som medfører at navigatørene har et tilstrekkelig vurderingsgrunnlag for å foreta hensiktsmessige beslutninger.

Bilde 1: Havarert vannscooter med fører på dekket til Nordnes. En lykkelig utgang.



Figur 1: Sosioteknisk Systemmodel. Human Factors In The Maritime Domain.

I følge den sosiotekniske systemmodellen illustrert i boken *Human Factors In The Maritime Domain*, (Grech, Horberry, & Koester, 2008)representerer individet en faktor. Det samme gjør teknologi. I følge boken er synet den viktigste sansen vi mennesker benytter til å tegne et bilde av en situasjon vi er en del av. Boken hevder videre at det er utviklet en del teknologisk utstyr som kan demme opp for ulemper som synet har. Mennesket har blant annet utfordringer med å se i mørket. I denne forbindelse er det blant annet utviklet radar og kameraer, som utnytter infrarød teknologi. Med andre ord konstrueres teknologi for å hjelpe mennesker med operasjoner selv om synet ikke vil fungere optimalt under gitte forhold, slik som i mørket. I denne overgangen mellom individ og teknologi ligger mange fallgruver og en av disse kan være at for mye informasjon presenteres på en skjerm samtidig, eller at innstillingene på systemet ikke understøtter hensikten med selve systemet. Sett i dette perspektivet mener jeg navigatørene i Sjøforsvaret kan være lite kritisk til innstillingene som benyttes på radar. Radaren hadde som utgangspunkt å detektere andre fartøy og ble brukt ifm avstandsretting av artilleri. I dag er radaren trolig det viktigste navigasjonshjelpemiddelet på skip. Men den må brukes riktig.

Situasjonsforståelse

Tilbakemeldingene som vi gir i forbindelse med mønstring kritiserer ofte navigasjonsteamene for ikke å være bevisste nok på de innstillingene som er på radaren når de går på vakt. Det være seg i forhold til hvordan farvannet og hvordan været endrer seg. Selv om vi har all verdens teknologi vil det ikke kunne hjelpe navigatøren hvis han ikke er i stand til å vurdere tilgjengelig informasjonen, og på bakgrunn av den treffe adekvate beslutninger som fører til fornuftige handlemønstre. For at en vaktsjef hele tiden skal kunne skaffe seg et godt nok bilde, er det behov for struktur. Denne strukturen tilstreber vi i Sjøforsvaret å knytte opp mot et begrep vi kaller «faser i navigasjon» (NAVKOMP, 2018). Disse fire fasene er forberedelsesfasen, turnfasen, kontrollfasen og transittfasen. Jeg mener at disse fasene kan knyttes opp mot Boyds beslutningssirkel (Richards, 2005). I de ulike fasene er det behov for både radar og kikkert ved navigering i mørket. I tillegg til beslutningssirkelen er navigatøren avhengig av å tilegne seg situasjonsbevissthet. Begrepet situasjonsbevissthet kan være vanskelig å få has på men jeg velger å illustrere Endsley sin måte å presentere situasjonsbevissthet på (Endsley, 1995a). Hun hevder situasjonsbevissthet handler om tre forskjellige nivåer representert som følger:

Nivå 1: Oppdage
Nivå 2: Forstå
Nivå 3: Predikere

På Nivå 1 har navigatøren behov for å oppdage relevant informasjon som er nødvendig for å kunne gjøre fornuftige vurderinger og fatte riktige beslutninger. Nivå

2 handler om å integrere forskjellig informasjon fra nivå 1 for å oppnå en helhetlig forståelse av omgivelsene og kan relatere dette til egne hensikter. Det tredje og høyeste nivået bygger på de to første og handler om å kunne predikere hendelser som kan skje i nær fremtid som kan ha eller ikke ha en innvirkning på egne handlemønstre (Endsley, 1995a).

Det er allerede nå verdt å nevne at en vaktsjef er avhengig av Nivå 1 for å kunne komme videre til Nivå 2 og Nivå 3. Forskning har vist at over 70% av alle ulykker oppstår fordi Nivå 1 ikke blir innfridd, altså har ikke vaktsjefen oppdaget viktig informasjon og kan derav ikke forstå noe, og heller ikke være i stand til å kunne forutsi om informasjonen kan ha betydning for egen situasjon i fremtiden.

Basert på denne teorien bør en navigatør i dagens informasjonsbaserte og teknologistyrte arbeidsposisjon ha evnen til å tolke den informasjonen som er nødvendig for å kunne gjennomføre egne operasjoner innenfor nødvendige sikkerhetsmarginer. Nøkkelen er å tilegne seg nødvendig informasjon. Basert på teorien om at nærmere 80 prosent av alle ulykker oppstår fordi den nødvendige informasjonen ikke registreres og dermed ikke blir tatt med i vurderinger, må våre vaktsjefer bli mer bevisst på innstillinger som settes på systemer og sensorer.

Radar

I mørket er radaren det desidert viktigste hjelpemiddelet for å unngå å seile på mørklagte objekter som er i sjøen. Radar er en forkortelse for «RAdio Detection and Ranging» og ble implementert i sjøfarten som et antikollisjonsverktøy. Antikollisjon er nettopp radarens aller viktigste oppgave og for at vi skal kunne hente ut adekvat informasjon til riktig tid, må personell som opererer den ha nødvendig kompetanse og riktige holdninger til hvilke innstillinger radaren skal ha for å tjene formålet. Dette skal ikke være noen leksjon i radarteori men snarere en påminnelse om de radarparameterne som er viktig å ha et forhold til. Disse er i tilfeldig rekkefølge (SNP 500, NAVKOMP 2013):

1. Antennerotasjonsperiode
2. Pulslengde
3. Gain
4. Anticlutter Sea
5. Anticlutter Rain
6. Skala
7. Syntetisk overlay
8. Frekvens

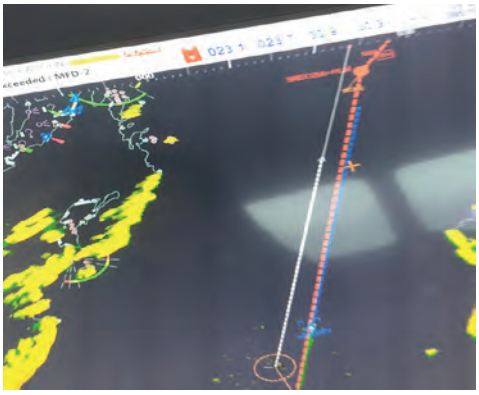
Antennerotasjonsperiode og pulslengde er de parameterne som avgjør hvor mye energi som blir sendt ut fra radaren mot et mål. Dette innebærer at en vil sende mer energi i et mål med lavere rotasjonshastighet. Samtidig vil energien bli redusert hvis pulslengden reduseres. For å oppdage ekko på lang avstand vil det være en fordel med lang puls og redusert rotasjonshastighet på antennen. Ulempen er redusert oppdatering på ekko og redusert oppløsning. Ved bare så vidt å komme innom de to første parameterne, er det lett å se at det må foretas bevisste valg av innstillinger basert på ytelsen vi ønsker tilpasset vår situasjon. For to Skjoldklassefartøy som møter hverandre i 60 knop, altså en relativ hastighet på 120 knop, vil det være lite gunstig med lav antennerotasjonshastighet som gir mindre hyppige oppdateringer av fartøysekkoene.

Ved hjelp av funksjonene gain, anticlutter rain og anticlutter sea er det mulig å manipulere den reflekterte energien som forenklet ble generert av pulslengden og rotasjonshastigheten på antennen. Ved hjelp av gain funksjonen kan presentasjonen på skjermen av den reflekterte energien forsterkes eller svekkes. Ved å skru gain helt ned forsvinner alle ekko fra skjermen og ved å øke den maksimalt blir skjermen gjerne helt gul. Ingen av de nevnte innstilligene vil presentere den informasjonen som er nødvendig for å gi et hensiktsmessig beslutningsgrunnlag. Dermed må også gain funksjonen få tilstrekkelig oppmerksomhet fra navigatøren og den må justeres i forhold til farvannets beskaffenhet. I et område med mye masse tett på fartøyet som reflekterer energi må gain justeres ned. Hvis ikke vil bildet bli meget uryddig og det vil være umulig å skille ut viktig informasjon. Videre kan en ytterligere dempe energien som er presentert på skjermen med sea clutter og rain clutter funksjonene. Clutterfunksjonene må benyttes med omhu da feil bruk regelrett kan skjule eller fjerne viktig informasjon

Valg av skala endrer naturligvis rekkevidden som radaren opererer på, men den endrer også oppløsningen ved at pulslengden endres automatisk i skjæringen mellom gitte skalaer. Vår evne til å oppdage detaljer blir redusert jo større skala det opereres på. Hvis radaren blir stilt inn på for stor skala i trangt farvann er det vanskelig å oppdage nye ekko som kommer ut fra en holme. Slik er det mulig å tenke seg svært mange scenarier hvor den ene eller andre innstillingen tjener eller ikke tjener den hensikten vi ønsker. Navigasjonsskala blir gjerne karakterisert fra 1,5nm og nedover for å ha en tilstrekkelig oppløsning på radarbildet.

«Information overload»

Nye brosystemer er integrerte, noe som medfører at informasjon fra mange sensorer kan presenteres på en eller flere skjermer. Et syntetisk bilde kan presenteres på radarskjermen etter ønske. Noen eksempler kan være en eller flere parallellindekser, bauglinjen, kurs over grunn linjen, en eller flere elektroniske peilelinjaler, flere avstandsringer, ruter og kart fra ECDIS kan legges oppå radarbildet med for eksempel lyktesektorer synlige. Dette illustrerer at navigatøren har mange muligheter til å gjøre



Bilde 2: Ikke lett å se ekkoet under det syntetiske bildet. Ekkoet i nedre høyre billedkant er derimot lett å oppdage.

Bilde 3: Kajakk delt i to av annet fartøy. Dagbladet.no

bildet uoversiktlig og til liten hjelp i beslutningsprosessen.

Felles for alle radarparameterne er at de kan være dynamiske og/ eller valgbare. Noen endrer seg ved at en annen parameter endrer seg. Et eksempel på dette er at pulslengden automatisk endrer seg i overgangen mellom spesifikke skalaer. Dette stiller store krav til navigatørens kompetanse og det stiller store krav til hensiktsmessige og bevisste innstillinger tilpasset situasjonen hjelpemiddelet skal tjene. Da alle parameterne er dynamiske, er det lett å tenke seg at uheldige innstillinger på flere parametere kan få dramatiske følger, slik det kunne blitt for personen på vannscooter en mørk høstdag i oktober.

For mange navigatører kan situasjonen som her beskrives virke søkt, men hvis denne tanken streifer en som navigatør, er min oppfatning at holdningene til problemstillingen kanskje er feil og profesjonaliteten i rollen som vaktsjef bør muligens revurderes. I 2016 ble en kajakk delt i to av et annet fartøy. Det var riktignok en fritidsbåt, men det kunne like gjerne vært et av våre fartøy, akkurat slik det kunne vært meg denne ene høstdagen eller en Skjold klasse som passerte en kajakk uten at den var detektert. Sett i lys av at nordmenn stadig mer trekker ut i naturen og det dermed blir flere kajakker, vannscootere og småbåter på sjøen er det essensielt at vi gjør det vi kan for å unngå ulykker. Holdningsendringer og regelendringer kommer ofte etter tragiske ulykker med døden som konsekvens. Dette er på mange måter en oppfordring til skipssjefer, vaktsjefer og navigatører generelt om å ta innstillinger på hjelpemidler seriøst. Når det er så mange innstillinger å velge mellom, stiller det større krav til navigatørene om å ta bevisste valg. Det ligger selvsagt også et ansvar i organisasjonene og utdanningsinstitusjonene for å påpeke disse utfordringene i opplæringen. Hvis en ulykke oppstår kan en bli dømt for uaktsomhet med de konsekvensene det innebærer. Skyldfølelse og ettervirkninger må håndteres og det er ikke sikkert at det er håndterbart og dermed må vi som navigatører være bevisst i den rollen vi påtar oss som vaktsjefer.

Vi må bli flinkere til å utnytte systemer etter hensikten

Så hva er det jeg egentlig prøver å påpeke? Mange navigatører i Sjøforsvaret må ta tak i egen bevissthet. Ikke bare få en vaktoverlevering og gå på vakt uten å være bevisst på om det utstyret du har tilgjengelig tjener formålet. Sjekk radarens ytelse mot objekter. Hvilke innstillinger gir best bilde i forhold til vær og situasjon? Bygg nye erfaringer på hver vakt og del erfaringene med kollegaer og organisasjon. Ikke overlat til tilfeldigheter at vaktsjefen du avløste hadde fornuftige innstillinger. Sjekk det ut og sørg for at du har de innstillingene du mener er hensiktsmessige. Vær sikker på at du har et godt argument for å seile med de innstillingene du har. Ved å ta bevisste valg som kan argumenteres for er vi kommet langt på vei mot å unngå nye tragiske ulykker. Det gjelder jo egentlig for alt vi gjør, men mitt formål med denne artikkelen handlet om bevisste innstillinger på systemene vi bruker, her illustrert gjennom radaren. For fartøy som har både x- band og s- band radar er det min klare oppfordring å seile med en av dem med så lite syntetisk clutter som overhode mulig. I tillegg må skalavalget være meget bevisst. Skalavalg og bruk av 3cm radar som gir best oppløsning bør vurderes opp mot sikker fart og fartøyets stoppedistanse. Jeg er ganske sikker på at ved bruk av kikkert vil en person stille på den hvis bildet er uklart. På lik linje med dette må radaren justeres slik at den yter optimalt sett opp mot deteksjon av mørke objekter og dermed unngå kollisjon med andre fartøy eller grunnstøting. Hensiktsmessige innstilinger kan i ytterste konsekvens redde liv.

Et annet aspekt er å ha et bevisst forhold til organisering og struktur av navigasjonsteamet vi leder som

vaktsjefer. Det er i mange tilfeller nødvendig med eksplisitt koordinering og rolleavklaring, slik det var for min egen del denne mørke høstkvelden nord for Fleslandskjæret lykt. Det er nødvendig å ha et bevisst forhold til den ytelsen vi ønsker å ta ut av et menneske, på lik linje med den ytelsen vi ønsker fra det utstyret vi utnytter, men det er et annet tema.

Referanser

Endsley, M. (1995a). Toward a theory of situation awareness in dynamic systems. *Human Factors, 37*, 32-64.

Grech, M., Horberry, T., & Koester, T. (2008). *Human Factors in the Maritime Domain.* Boca Raton: CRC Press.

NAVKOMP. (2018). *SNP 500, Reglement for utøvelsen av militær navigasjon på Forsvarets fartøyer.* Sjøforsvaret. Bergen: Sjef Sjøforsvaret.

Richards, C. (2005). *Certain to Win* (2 ed.). J. Addams & Partners, Inc.

Kyst- og innaskjærs navigasjon – digitalisert

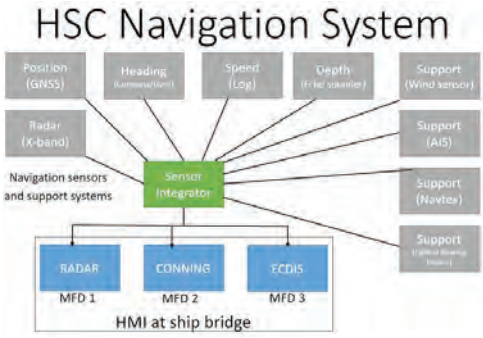
Odd Sveinung Hareide

Sammendrag

Sjøforsvaret har en lang tradisjon av å benytte seg av den norske skjærgården for å skaffe en operativ fordel mot fienden. Dette innebærer blant annet å kunne navigere effektivt i krevende kyst- og innaskjærs farvann. Det siste tiåret har Sjøforsvarets fartøy blitt digitalisert, elektronisk navigasjon har blitt innført. Denne artikkelen gir en kort oversikt over Sjøforsvarets Navigasjonskompetansesenterets erfaring med og bruken av elektronisk navigasjon i en krevende skjærgård.

Kyst- og innaskjærs navigasjon

Det tradisjonelle navigasjonshåndverket har stått sterkt i Sjøforsvaret, blant annet vist ved at faget «Militær Praktisk Navigasjon» tar en betydelig del av studietiden til kadettene ved Operativ Marinelinjen (dekksoffisersutdanning). Manuelle posisjoneringsmetoder blir undervist og praktisert gjennom en modulbasert opplæring, og det legges mye ressurser i praktisk gjennomføring enten i simulator eller med skolefartøy (1). Sjøkrigsskolen har publisert egne håndbøker som tar for seg kyst- og innaskjærs navigasjon (2), samtidig som en har arbeidet med å forene dette med den teknologiske utviklingen gjennom reglement for utøvelse av elektronisk navigasjon (3).



Figur 1: Eksempel på navigasjonssystem med integrasjon mot ulike sensorer.

Elektronisk navigasjon

Den teknologiske utviklingen har bidratt til at navigatøren i dag benytter tiden til å monitorere posisjonen som blir presentert på det integrerte navigasjonssystemet, i motsetning til tidligere ved bruk av papirkart når det til tider var krevende å finne og angi posisjonen til fartøyet. Hovedårsaken til at en i dag kan monitorere posisjonen, er at det elektroniske kartet er integrert mot posisjonssensorer som presenterer fartøyets posisjon nesten i sann tid.

Den mest benyttede posisjonssensoren er GPS, og det er viktig for navigatøren å kjenne til muligheter og begrensningene med alle navigasjonssensorene som benyttes i det integrerte navigasjonssystemet (4).

Det tradisjonelle håndverket med grundig planlegging og kontinuerlig kontroll med fartøyets posisjon er like aktuelt i dag som tidligere, forskjellen er at kontrollen i dag skjer gjennom digitale display. Navkomp har tidligere gjennomført simulatorforsøk som viser at

trente navigasjonsteam i Sjøforsvaret har stor tillit til posisjonen som presenteres fra posisjonssensorene, og det har vært en bekymring for at navigasjonsteamet stoler for mye på navigasjonssystemet, som kan inneha feil (playstation-mode) (5). Et viktig aspekt ved innføringen av digitale systemer til hjelp for navigatøren, er at navigatøren nå også må forstå mulighetene og begrensningene i dette systemet for å opprettholde en høy situasjonsbevissthet (SA), angitt ved høy grad av systemforståelse (system awareness).

Figur 3: Elementer i navigatørens situasjonsbevissthet (6).

Forening av tradisjonelle navigasjonsprinsipp og digitale hjelpemiddel

En gjentagende tilbakemeldinger fra moderne fartøy, er at det er for mange display og utstyr på broen (7), og det er ønskelig med enkelthet i design og layout av de digitale hjelpemidlene til navigatøren.

Navkomp arbeider kontinuerlig sammen med systemleverandørene for å tilrettelegge for kyst- og innaskjærs navigasjon på elektroniske kartsystemer (ECDIS). Eksempel på dette er utvikling av nytt rutemonitoreringsvindu (Figur 4) og videreutvikling av terrestrisk posisjonssensor, samtidig arbeides det med å få tilgjengelig relevant informasjon for navigatøren hos andre systemleverandører.

Figur 4: Nytt high speed rutemonitoreringsvindu i Kongsberg sin software (8).

Tradisjonelle navigasjonsprinsipper som planlegging og kontroll av seilas må være enkelt å gjennomføre på det integrerte navigasjonssystemet, samtidig som grensesnittet mot navigatøren må være enkelt. Som et eksempel viser et forskningsprosjekt fra Navkomp at når ny software og grensesnitt ble presentert for navigatøren, benyttet en navigatør som er kjent med dette grensesnittet 41% mer av tiden på å kontrollere omgivelsene rundt fartøyet (SE UT!) (9).

Table 2. Comparison of the most experienced participant in the two data sets.

Data set/AOI (%)	Outside	ECDIS	Route monitor	Radar	Conning
Pre mid-life update	70%	14%	8%	3%	5%
Post mid-life update	68%	21%	9%	1%	1%

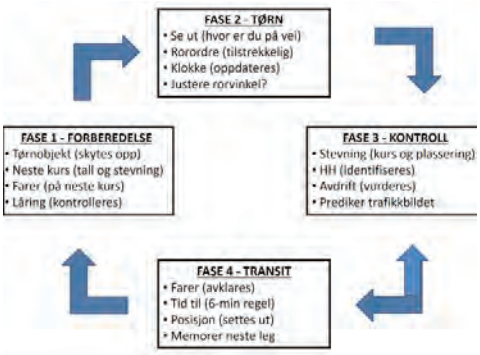
Table 3. Comparison of the least experienced participant in the two data sets.

Data set/AOI (%)	Outside	ECDIS	Route monitor	Radar	Conning
Pre mid-life update	47%	29%	10%	5%	9%
Post mid-life update	27%	49%	21%	1%	2%

Figur 5: Sammenligning av erfaren og uerfaren navigatør på ny software (grensesnitt) (9).

Prosedyrer og metodikk

Metodikken i Sjøforsvaret er kjent som faser i navigasjon (10), og kan anses som en beslutningssirkel som må lukkes innen den starter på nytt, med andre ord er tid essensielt.



Figur 6: Faser i navigasjon

Prosedyrer for kommunikasjon henger sammen med fasene i navigasjon, og det er på de fleste fartøystyper etablert prosedyrer for brokommunikasjonen som sammenfaller med fasene i navigasjon. Det neste steget er nå å få designet av det elektroniske navigasjonssystemet til å understøtte dette, noe vi foreløpig kun har til en viss grad på Skjold-klassen (8, 11).

Standardisering

Sjøforsvaret sammen med FMA arbeider for en standardisering av navigasjonssystemene som er i bruk i Sjøforsvaret. Per i dag er det fem større leverandører av integrerte navigasjonssystemer, og Navkomp anbefaler å forholde seg til to leverandører for å forenkle undervisning, opplæring, praktisk trening og standardisering av prosedyrer i Sjøforsvaret.

Konklusjon

Prinsippene for kyst- og innaskjærs navigasjon benyttet i papirkartets tid er fortsatt like relevante, og det vil nå arbeides for at det integrerte navigasjonssystemene om bord på Sjøforsvarets fartøy tilpasses for militær navigasjon. Navigatører på Sjøforsvarets fartøy må være bevisst mulighetene og begrensningene i navigasjonssystemet de benytter, for til enhver til å opprettholde sikker og effektiv navigasjon gjennom høy grad av situasjonsbevissthet.

Referanser

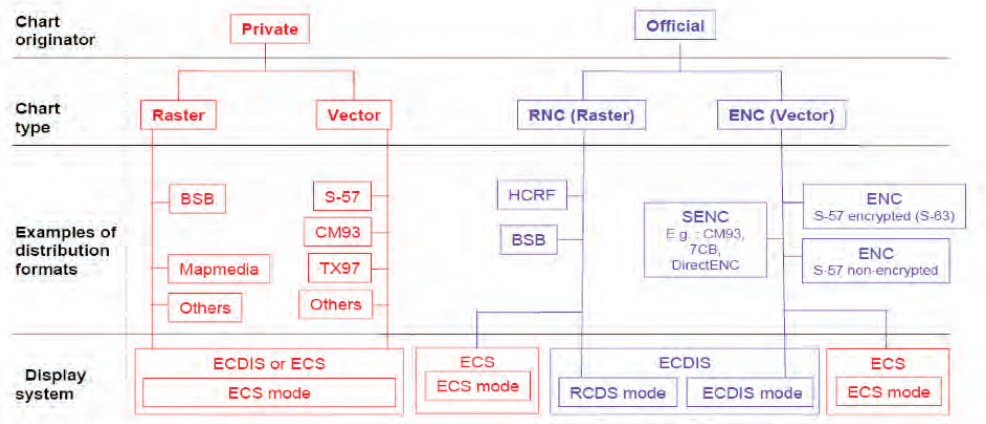
1. Hareide OS, Nyhamn S. Militær navigasjon - en krevende oppgave / 24/7 readiness. NAVIGARE. 2016:32-8.
2. Øi Ø. Kyst- og innaskjærs navigering i Marinen. Bergen: John Grieg AS; 1993. 86 p.
3. Sjøforsvaret. SNP-500 In: Navigasjonskompetansesenter S, editor. Bergen2018.
4. Glomsvoll O, Bonenberg LK. GNSS jamming resilience for close to shore navigation in the Northern Sea. The Journal of Navigation. 2017;70(1):33-48.
5. Hareide OS. Kontroll av ECDIS. Norsk Tidsskrift for Sjøvesen. 2014:11-7.
6 Hareide OS, Jøsok Ø, Lund MS, Ostnes R, Heikala K. Enhancing Navigator Competence by Demonstrating Maritime Cyber Security. Journal of Navigation. 2018; Accepted, in publication.
7. Fagerholt RA, Kongsvik T, Moe HK, Solem A. Broutforming på hurtigbåter. Kartlegging av problemer med utforming og funksjonalitet på teknisk utstyr på hurtigbåt-bro. Rapport. NTNU Samfunnsforskning AS; 2014.
8. Hareide OS, Mjelde FV, Glomsvoll O, Ostnes R, editors. Developing a High-Speed Craft Route Monitor Window. International Conference on Augmented Cognition; 2017: Springer.
9. Hareide OS, Ostnes R, editors. Validation of a Maritime Usability Study with Eye Tracking Data. HCI International; 2018; Las Vegas: Springer.
10. Hareide OS, Ostnes R. Scan Pattern for the Maritime Navigator. Transnav. 2017;11(1):39-47.
11. Hareide OS, Vågenes S. Operativ FoU - et eksempel. Necesse. 2017;2(1):5.

Utvikling av elektroniske sjøkart

Odd Sveinung Hareide, Fagleder Elektronisk Navigasjon, Sjøforsvarets Navigasjonskompetansesenter
Mette Karlsen, Gruppeleder ENC produksjon, Kartverket Sjødivisjonen

Sammendrag

I løpet av de siste årene har de fleste av Sjøforsvarets brukere gått over fra papirkart til elektroniske kart. Flere har ytret bekymring overfor utfordringer med bruk av elektroniske kart, som ikke var tilstede med papirkart. I tillegg har elektroniske kart tilført noe som papirkart ikke hadde, for eksempel større detaljgrad. Sjøforsvaret og Kartverket Sjødivisjonen har over noen år jobbet målrettet med å videreutvikle det elektroniske kartet, og denne artikkelen viser til noen eksempler på dette.



Picture 5: Examples of Electronic Chart Formats. Many ECS systems are able to use ENC or RNC data, however even when using official charts they may not be used to fulfil carriage requirements.

Elektroniske sjøkart

Electronic Navigation Charts (ENC) er internasjonalt anerkjent betegnelse for godkjente offisielle elektroniske sjøkart. Kartverket sjødivisjonen produserer og oppdaterer Norge sine ENCer. Det er viktig å skille mellom ulike typer kart, og figuren under illustrer denne forskjellen.

En ENC er et vektorkart som skal inneholde all informasjon som er nødvendig for å gjennomføre en sikker seilas. Disse elektroniske sjøkartene er fremstilt på bakgrunn av standarden som er utviklet av den internasjonale hydrografiske organisasjon (IHO) for utveksling av digital sjøkartinformasjon, kjent som S-57.

ENCer brukes til papirløs navigasjon i en ECDIS eller en ECS, og dette gir navigatøren mulighet til en sømløs presentasjon av de elektroniske sjøkartene med sanntidsposisjonering ved bruk av for eksempel GPS.

ENC Improver

ENC Improver er et web-basert tilbakemeldingssystem for offisielle norske elektroniske sjøkart, og er utviklet for å gi brukerne et enkelt system for tilbakemelding på de norske ENC-ene. Tilbakemeldinger fra brukerne er til hjelp i arbeidet med å holde ENC-ene mest mulig oppdatert, og er dermed et viktig bidrag for at sikkerheten til sjøs ivaretas.
ENC Improver benyttes for å melde inn feil, mangler eller ønsker om forbedring i de norske ENC-ene.
Alle som har en ENC-lisens for navigasjon vil få brukertilgang til ENC Improver via sin leverandør, og tilgangen er beskrevet i mailen hvor permits er tilsendt.

Funksjoner i ENC Improver er:
- Kartløsning (peke i kart og beskrive)
- Posisjon (gi inn koordinater og beskrive)
- Generell tilbakemelding på ENC-er
- System for oppfølging av innmeldt sak

Stevningsobjekt

I papirkart var for eksempel kirker og enkelte stevningsobjekter som ble brukt tegnet inn, noe som til en viss grad har forsvunnet i det elektroniske sjøkartet. Her har vi gode muligheter til å melde inn behov til Kartverket Sjødivisjonen via ENC Improver, og et eksempel er høyblokken i Gravdal. Denne høyblokken er et godt stevningsobjekt når en skal seile i Byfjorden, og er tegnet inn som vist i bildet under.

Andre eksempel Sund Kirke ved Klokkarvik, som har vært et godt stevningsobjekt i papirkart 21 som er borte i det elektroniske kartet. I 2018 er det gjennomført en bacheloroppgave som tar for seg forskjellene på informasjonspresentasjon i papirkartet og det elektronisk sjøkartet i området rundt Bergen (kart 21 og 23).

Elektroniske sjøkart rundt Svalbard

Kartgrunnlaget vil for mange områder være basert på sjømålingsdata hvor posisjonsnøyaktigheten er dårligere enn det som i dag er mulig ved bruk av moderne posisjoneringssystemer. Det samme gjelder for dekningsgraden, der eldre målinger med eldre innmålingsutstyr (ekkolodd) ikke gir et fulldekkende bilde av havbunn som ved bruk av moderne utstyr. I en ENC er datakvaliteten for hydrografiske data angitt i kvalitetssoner (Zones of Confidence – CATZOC, også betegnet som Data Quality) hvor kvaliteten er vurdert ut fra tre faktorer:

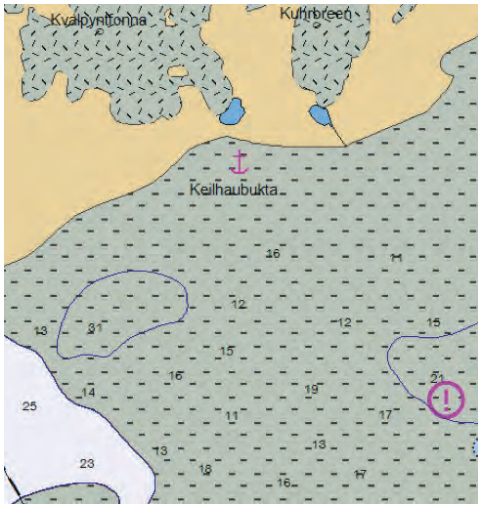
1. Posisjonsnøyaktighet
2. Nøyaktighet i dybde
3. Dekningsgrad av havbunnen

Kvalitetssonene er beskrevet i figuren på side 48.

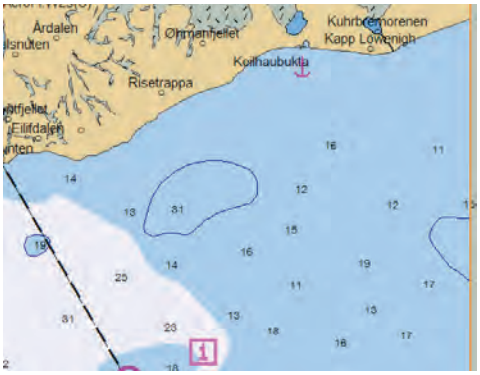
Rundt Svalbard er mange ENC-er basert på digitaliserte overseilingskart. Disse kartene har store områder som er definert som ikke-sjømålt i kildediagrammet, men som allikevel inneholder noen usikre dybdekurver og dybdepunkt. Dette er data vi ikke kjenner kilden til og kvaliteten på dybdeangivelsene er derfor svært usikker. Når disse områdene kodes likt i ENC som i papirkartene blir dybdeinformasjonen vanskelig å lese i ECDIS på grunn av S-52 presentasjon. Etter tilbakemelding fra Kystvakten har Kartverket Sjødivisjonen endret praksis. Sjødivisjonen vil nå legge inn dybdeareal der det finnes batymetri i de ikke-sjømålte områdene. Som minimum dybdeverdi legges det inn 0 m. Maksimum dybdeverdi vurderes ut ifra innholdet av kurver og dybdepunkt i gjeldende område. Istedenfor ikke-sjømålt areal vil områdene da framstå som farlig areal i ECDIS, og batymetrien vil være lesbar. Datakvalitet vil fortsatt være dårlig (CATZOC D).

Her er eksempler fra to steder hvor dette er gjennomført:

Sør for Edgeøya, ca pos N 77:25 E 21:37

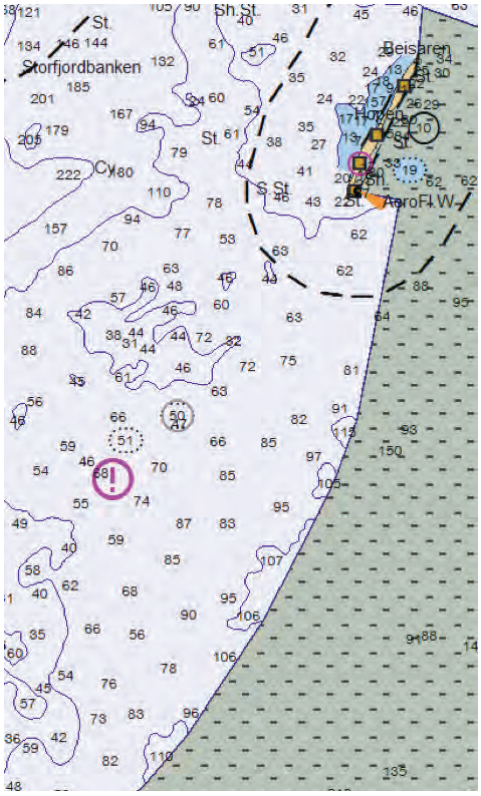


NO2A4436: Unsurveyed area - Compilation Scale 700 000



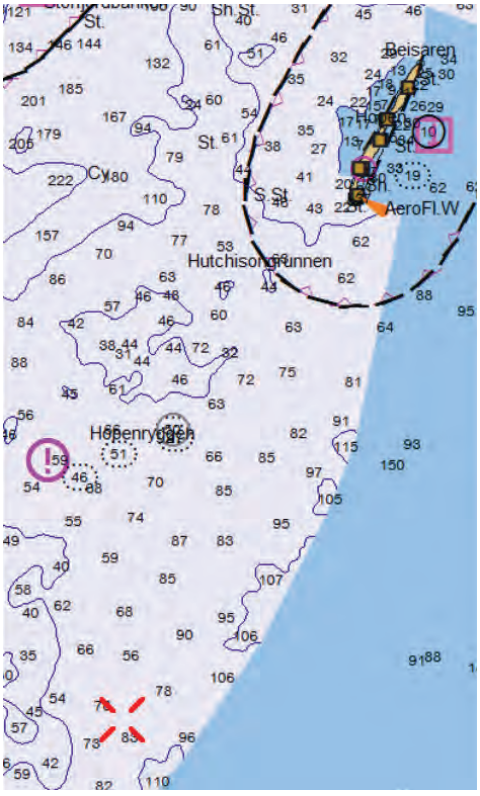
NO3C4436: Samme område, men Unsurveyed area er erstattet med et dybdeareal 0m-50m. Compilation Scale 90 000

I ECDIS vil en se NO2A4436 med Unsurveyed area når man er zoomet langt ut, og når man zoomer inn til NO3C4436 vil en se dybdeareal.



Sør for Hopen, ca pos N 75:30 E 25:30
NO2A4036 - Compilation Scale 700 000

Før: «Unsurveyed area» strekker seg fra Hopen og sørover



Etter: «Unsurveyed area» er erstattet med dybdeareal 0m–300m

ZOC Category

1	2	3	4	5
ZOC[1]	Position Accurancy[2]	Depth Accurancy[3]	Seafloor Coverage	Typical Survey Characteristics[5]
A1	± 5 m + 5% depth	= 0.50 + 1%d Depth (m): 10, 30, 100, 1000 Accurancy (m): ± 0.6, ± 0.8, ± 1.5, ± 10.5	Full area search undertaken. Significant seafloor features detected[4] and depths measured.	Controlled, systematic survey[6] high position and depth accuracy achieved using DGPS or a minimum three high quality lines of position (LOP) and a multibeam, channel or mechanical sweep system.
A2	± 20 m	= 1.00 + 2%d Depth (m): 10, 30, 100, 1000 Accurancy (m): ± 1.2, ± 1.6, ± 3.0, ± 21.0	Full area search undertaken. Significant seafloor features detected[4] and depths measured.	Controlled, systematic survey[6] achieving position and depth accuracy less than ZOC A1 and using a modern survey echosounder[7] and a sonar or mechanical sweep system
B	± 50 m	= 1.00 + 2%d Depth (m): 10, 30, 100, 1000 Accurancy (m): ± 1.2, ± 1.6, ± 3.0, ± 21.0	Full seafloor coverage not achieved; uncharted features, hazardous to surface navigation are not expected but may exist.	Controlled, systematic survey achieving similar depth. But lesser position accuracies than ZOCA2, using a modern survey echosounder[5], but no sonar or mechanical sweep system.
C	± 500 m	= 2.00 + 5%d Depth (m): 10, 30, 100, 1000 Accurancy (m): ± 2.5, ± 3.5, ± 7.0, ± 52.0	Full seafloor coverage not achieved, depth anomalies may be expected.	Low accuracy survey or data collected on an opportunity basis such as soundings on passage.
D	worse than ZOC C	worse than ZOC C	Full seafloor coverage not achieved, large depth anomalies may be expected.	Poor quality data or data that cannot be quality assessed due to lack of information.
U	Unassessed – The quality of the bathymetric data has yet to be assessed			

Konklusjon

På tross av at vi har benyttet elektronisk navigasjon og ENCer over en lengre periode, så er det fortsatt et produkt under utvikling. Kartverket Sjødivisjonen jobber aktivt mot IHO for å få bedre informasjonspresentasjon, og de ønsker innspill fra brukerne. Sjøforsvaret er en aktiv bruker av den norske kystlinjen, og ved å benytte ENC Improver har vi gode muligheter for å delta i videreutviklingen av ENCene. Som en del av Kongeriket Norge har Sjøforsvarets fartøy et spesielt ansvar for å støtte Kartverket i rapportering og videreutvikling av sjøkartene langs norskekysten. Kartverket Sjødivisjonen og Sjøforsvarets Navigasjonskompetansesenter vil fortsette det gode samarbeidet for å forbedre det elektroniske sjøkartet til fordel for sluttbrukeren i den spisse ende.

S-102: Fremtidens navigasjon

Odd Sveinung Hareide, Fagleder Elektronisk Navigasjon, Sjøforsvarets Navigasjonskompetansesenter.
Sølvi Tunge, Electronic Chart Centre

Sammendrag

Med elektroniske kart kommer både muligheter og begrensninger. I S-102 prosjektet ser samarbeidspartnerne på fremtidens navigasjon, og hvordan en kan benytte seg av stadig større datamengder for å presentere kartrelatert informasjon for å øke situasjonsbevisstheten til operatøren. S-102 prosjektet vil gjennomføre en demonstrator med bruk av 3D-kart, der bruken av de skal evalueres i henhold til oppdraget som skal gjennomføres. Dette vil kunne bidra til økt sikkerhet og bedre utnyttelse av farvannet, og kan tilføre økt operativ nytte.

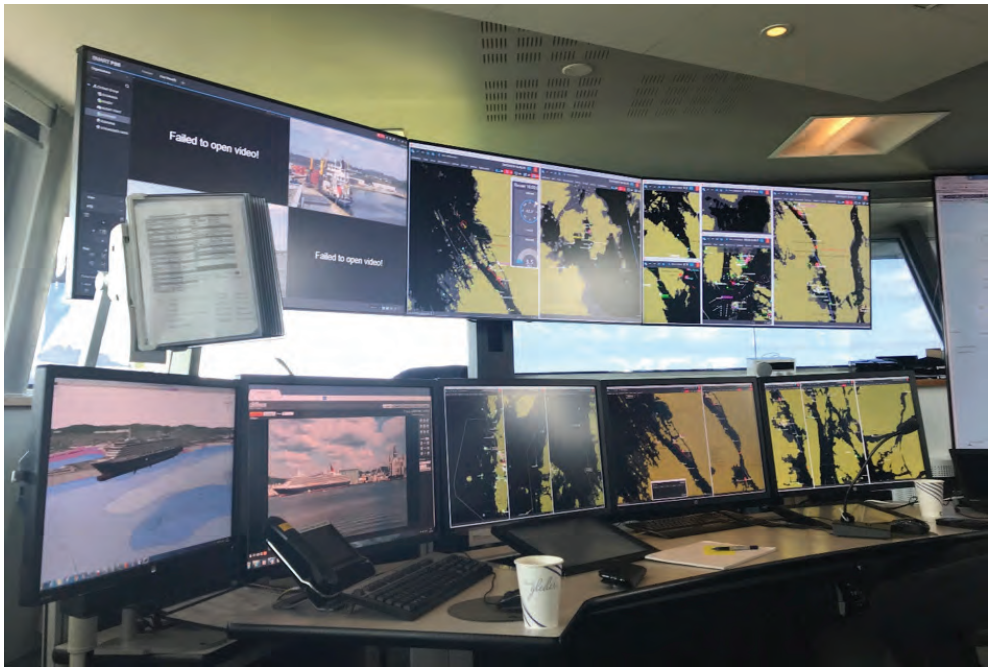
Den norske maritime næringen er internasjonalt ledende på mange felt. Et overordnet mål for sjødivisjonen i Kartverket er, på en kosteffektiv måte, å tilgjengeliggjøre maritim geografisk informasjon som fremmer navigasjonssikkerhet og imøtekommer øvrige behov hos brukere og forvaltere av norske kyst- og havområder. Norge er også operatør for PRIMAR, et internasjonalt samarbeid for kvalitetssikring og leveranse av Elektroniske Sjøkart for navigasjon. Disse sjøkartene er produsert og levert i henhold til internasjonale standarder fra IHO (International Hydrographic Office). IHO jobber nå med en ny standard for dybdedata – S-102. Detaljerte dybdedata gir enorme muligheter og er etterspurt av mange maritime brukergrupper.

Et slikt datalag gir muligheter for nytenkning, verdiskapning og innovasjon rundt navigasjon og navigasjonsplanlegging. I tillegg vil det kunne gi samfunnsnyttig verdi innenfor andre områder som eksempelvis analyse, planlegging, beredskap og i forbindelse med ulykker. Det har i et par år vært jobbet med å få testet slike data i samspill med andre datakilder i et reelt brukermiljø. En stor begrensning har vært å få dataene distribuert og installert i et system for brukeren. Det er nettopp dette en gjennom prosjektet ønsker å få satt fokus og fortgang på.

Innovasjonen i prosjektet vil fokuseres rundt identifisering av muligheter rundt distribusjon av S-102 data samt utvikling av en demonstrator som kan teste og visualisere dataene i tett samarbeid med utvalgte brukergrupper. Verdiskapningen vil være at en gjennom en bedre forståelse av hvordan en kan ta i bruk dybdedata kan legge et bedre grunnlag for ressursbesparelse, miljøhensyn, reduserte kostnader, økt sikkerhet og økt effektivitet blant brukerne av kartdataene gjennom en mer helhetlig og dynamisk oversikt over sjøgrunnen. Gode løsninger for distribusjon vil sikre Norge sin internasjonalt ledende rolle i forbindelse med tilgjengeliggjøring av offisielle og autoriserte navigasjonsprodukter for fremtiden.

Electronic Chart Centre (ECC), Kartverket, Sjø/PRIMAR, Kongsberg Digital (KDI), Kystverket og FMGT jobber sammen i S-102 Demonstrator prosjektet finansiert av Forskningsrådet for å utvikle en tjeneste for distribusjon og bruk av batymetriske data (S-102) i operasjonelt miljø. I selve demonstratoren er S-102 sammenstilt med andre datalag som blant annet ENCs og land informasjon. I prosjektets første del har det blitt fokusert på utvikling av demonstrator basert på gode innspill og tilbakemeldinger med hensyn på behov for funksjonalitet direkte fra brukerne. I den neste og siste fasen er det fokus på distribusjonsmetoder, og bruken av selve demonstratoren i operasjonelle situasjoner. Prosjektets varighet er 2 år.

De påfølgende bilder og tilbakemelding er etter første operasjonelle test i prosjektet utført ved Kvitsøy



Figur 1: 3D kart tilgjengelig på Kvitsøy Sjøtrafikksentral vises på skjerm nede til venstre

Sjøtrafikksentral, hvor en fikk følge MS Queen Victoria sin avgang fra Haugesund gjennom Osnesgavelen og Skårerenna.

«Det å kunne følge fartøyet sin seilas i 3D kart øker sjøsikkerheten i område. Operatør har ved dette hjelpemiddelet mulighet til å forutse farer som kan oppstå og dermed informerer fartøyet før den vil oppstå. Dette kan være avstand under kjøl i forhold til dybde samt avstand sideveis til eventuelle farer. Demonstratoren er også et meget godt hjelpemiddel til å kunne oppgi en trygg ankerposisjon til fartøy som ønsker å ankre.» Asle Njåstad Trafikkleder Kvitsøy Sjøtrafikksentral.

Figur 2: Skjermdump fra S-102 verktøy.

S-102 prosjekts relevans for Sjøforsvaret

Sammen med ECC, Kartverket (Sjø/PRIMAR) og KDI gjennomføres en demonstrator for distribusjon og bruk av batymetriske data (S-102) i operasjonelt miljø. Sjøforsvarets Navigasjonskompetansesenter (Navkomp) stiller med fartøy og personell til å gjennomføre demonstratoren. Hensikten er å se på hvordan en bedre kan utnytte seg av 3D-kart i et operasjonelt miljø, samt hvordan en kan øke situasjonsbevisstheten til fartøyet/navigatøren og dermed også kunne bidra til sikker og effektiv navigasjon. Det vil spesielt ses på økt beslutningsgrunnlag i operasjoner under vann, samt planlegging i forkant og i gjennomføringen av taktiske forflytninger.

For mer informasjon se https://s102.no/

Det har også blitt skrevet en bacheloroppgave om relevansen av S-102 for Sjøforsvaret, den er tilgjengelig på forespørsel til Navkomp.

DEL 3

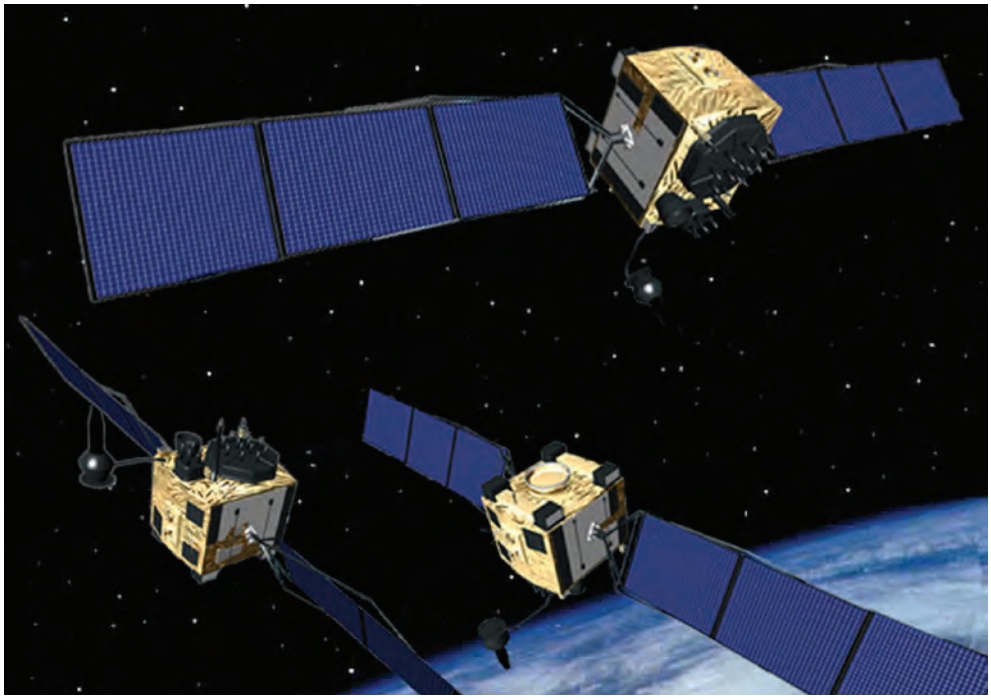
Teknologisk utvikling for effektiv navigasjon

Hvor nøyaktig er GPS?

Stein Egil Iversen

Sammendrag

NAVSTAR GPS er i dag det eneste GNSS-systemet som møter NATO-alliansens krav til nøyaktighet, robusthet, pålitelighet og tilgjengelighet for PNT-data. Forsvaret benytter derfor GPS som PNT-kilde for sine plattformer. For Sjøforsvarets vedkommende gir kontinuerlig posisjonsinformasjon grunnlag for høypresisjons navigasjon, men hvor nøyaktig er egentlig GPS?



Det enkleste svaret er "det spørs", siden posisjonsnøyaktigheten til GPS er avhengig av en rekke faktorer, og ikke er en absolutt verdi.

Verdensrommet, breddegrad og topografi

GPS inkluderer per mars 2018 31 operasjonelle satellitter[1]. Satellittene sender PNT-informasjon på to forskjellige bærefrekvenser som begge er i L-båndet: L1 på 1575, 42 MHz og L2 på 1227,6 MHz. PNT-informasjonen sendes med to forskjellige nøyaktighetsnivåer: SPS (Standard Positioning Service) og PPS (Precise Positioning Service). SPS PNT-informasjon er tilgjengelig for alle brukere mens PPS PNT-informasjon er forbeholdt militære brukere og er dermed kryptert. Tilgang til de militære signalene er regulert gjennom multilaterale avtaler mellom USA og medlemsnasjonene i NATO. De samme avtaler beskriver forpliktelsene USA har i forhold til å opprettholde tilgjengelighet og nøyaktighet.

Standarden for global gjennomsnittlig nøyaktighet til SPS er av det amerikanske forsvarsdepartementet angitt til å være ≤ 7,8 meter 95 % av tiden[2] mens standarden for PPS er ≤ 5,9 meter 95 % av tiden.[3] I begge tilfeller gjelder dette User Range Error (URE), som utgjøres av tidsfeil og banefeil til satellittene. I 2016 var global SPS URE ≤ 0,715 meter 95 % av tiden, mens PPS URE var ca. 0,5 meter. Den definerte nøyaktigheten gjelder dermed for signalene fra satellittene i verdensrommet og ikke posisjonen som vises på en GPS-mottaker.

Denne markante forbedringen av posisjonsnøyaktigheten på signalet i verdensrommet skyldes b.la. flere tilgjengelige satellitter samt økt antall GPS-monitoreringsstasjoner der sistnevnte gir grunnlag for oppdatering av satellittenes baner med nøyaktighet på centimeternivå. Banedataene er en del av navigasjonsmeldingen til satellittene og er delt inn i almanakk- (grove banedata) og efemeridedata (høyoppløselige data), og oppdateres typisk minst en gang i døgnet. Dersom banedata ikke oppdateres vil posisjonsnøyaktigheten gradvis reduseres.

I signalet fra satellittene ligger det i tillegg til informasjon om banedata for den enkelte satellitt, også informasjon om ionosfæriske- og troposfæriske forhold. Dette er dels basert på målinger og dels på matematiske modeller. Dersom modellene ikke er tilstrekkelig oppdaterte, vil dette kunne forårsake posisjonsfeil på opptil 10 meter. Forbedret modellering og måling har medført at påvirkningen minimeres.

Signaler fra satellitter med lav elevasjon vil gå en engre vei gjennom ionosfæren og troposfæren enn signaler fra satellitter med høyere elevasjon, og vil derfor bli mer utsatt for feil. GPS-satellittene har en inklinasjon til ekvator på 55° som innebærer lengre signalvei til mottakere på høye breddegrader som igjen medfører en større usikkerhet og dermed posisjonsfeil.

Operasjoner i fjorder eller andre farvann der signaler fra enkelte satellitter blokkeres av topografien, gjør at de satellitter som gir best geometrisk skjæring (DOP-verdier) ikke nødvendigvis kan inngå i posisjonsberegningen. Dette gir økt posisjonsfeil.

GPS-mottakeren og antennen

I undersøkelser foretatt i 2016[4] ble SPS posisjonsfeil på GPS-mottakere målt til mellom 1 og 2,5 meter. Testutstyret inkluderte to-frekvens GPS-mottakere, optimal antennekonfigurasjon og egne algoritmer designet for å minimere ekstern påvirkning på satellittsignalet. Alle målinger ble foretatt stasjonært, dvs. at mottakerne stod i ro. Måleresultatene er derfor ikke direkte sammenlignbare med ytelse til enkeltstående GPS-mottakere montert om bord på fartøy.

GPS-mottakere er designet i forhold til ett gitt bruksområde. Det er viktig at mottakeren passer til plattformen den skal anvendes om bord på for at brukeren skal få størst mulig ytelse. I de siste årene har prosessorkapasiteten i GPS-mottakere økt betraktelig og det er utviklet og implementert en rekke algoritmer som gjør at moderne mottakere gir PNT-informasjon med stor grad av nøyaktighet.

Alle typegodkjente maritime sivile GPS-mottakere følger ytelseskrav bestemt av IMO. Dette gir en definert minimum posisjonsnøyaktighet under spesifiserte forhold.

Militære GPS-mottakere som anvendes om bord er ikke underlagt de samme bestemmelsene som sivile. Selv om militære GPS-mottakere ikke er sertifiserte, vil de under normale mottaksforhold være like nøyaktig som sivile mottakere. I tillegg kan feil som skyldes ionosfæriske forhold ytterligere minimeres ved mottak på begge GPS-frekvensene. Militære mottakere kan videre fortsette operasjon ved større andel elektromagnetisk støy enn sivile mottakere, og er beskyttet mot spoofing når krypto er lastet.

GPS-antennen skal plasseres så høyt som mulig og på en slik måte at man i størst mulig grad unngår elektromagnetisk stråling og signalskjerming- eller refleksjoner (multipath) fra øvrige antenner og utstyr. Valg av kabel fra GPS-antennen og forlegging av denne frem til mottakeren skal være i henhold til gjeldende direktiver som omhandler elektromagnetisk interferens

---

[1] *https://www.gps.gov/systems/gps/space/*
[2] *Global positioning system standard positioning service performance standard 2008. Tilgjengelig på www.gps.gov*
[3] *Global positioning system precise positioning service performance standard 2007. Tilgjengelig på www.gps.gov*
[4] *An analysis of GPS SPS performance for 2016. Tilgjengelig på www.gps.gov/systems/gps/performance*

(EMI) og kompabilitet (EMC). De militære direktivene stiller større krav enn de sivile, og signalene til en militær GPS-mottaker vil dermed være bedre skjermet mot ytre elektromagnetisk påvirkning.

Ytelsesforbedring med differensiell GPS

Differensiell GPS (DGPS) baserer seg på at posisjonen som beregnes i en GPS-mottaker korreleres mot kjent posisjon slik at GPS-posisjonsfeilen kan bestemmes. Dette gjøres i bakkestasjoner. Korreksjonsverdiene for de enkelte satellittene (differensierte data) distribueres deretter fra bakkestasjonene til brukerne enten via radio eller via satellitt. Merk at DGPS kun gir korreksjonssignaler for det sivile GPS-signalet (SPS) og ikke det militære (PPS).

Langs norskekysten har Kystverket en DGPS-kjede bestående av 12 stasjoner som kringkaster korreksjonsverdiene over Kystverkets maritime radiofyr i frekvensbåndet 283,5 KHz til 315 KHz. For å motta disse signalene kreves det følgelig en radiofyrmottaker (beacon). Dette benevnes GBAS (Ground Based Augmentation System). Ved anvendelse av GBAS vil mottak av det differensielle korreksjonssignalet være avhengig av avstanden til radiofyrene, topografiske forhold, interferens fra andre radiosendere og støy forårsaket av nedbør.

De differensielle korreksjonssignalene kan også mottas via satellitt og benevnes da SBAS (Satellite Based Augmentation System). Bruk av SBAS kan enten skje via åpne tjenester eller kommersielle betalingstjenester. Posisjonsnøyaktigheten ved bruk av DGPS ligger typisk i området 1 – 3 meter for åpne tjenester. For kommersielle tjenester kan en nøyaktighet på desimeternivå oppnås.

Den åpne SBAS tjenesten i Europa er EGNOS (European Geostationary Navigation Overlay Service) som har 39 bakkestasjoner som via kontrollsentre og egne uplinkstasjoner sender signalene til geostasjonære satellitter som igjen kringkaster signalet til brukerne. Signalet sendes på GPS L1-frekvensen. For å nyttiggjøre seg signalet, må GPS-mottakeren kunne lese dette. Dette er implementert i majoriteten av typegodkjente maritime GPS-mottakere. Ved høye breddegrader vil EGNOS -satellittene ha en lav elevasjon som kan medvirke til at man ikke oppnår nevneverdig ytelsesforbedring, eller mister de differensielle korreksjonssignalene.

For nordamerikanske farvann er den åpne SBAS tjenesten WAAS (Wide Area Augmentation System). Oppbygging og distribusjon av signalene er tilsvarende som for EGNOS.

Anvendelse av DGPS må slås på i oppsettet på GPS-mottakeren. De fleste mottakere har funksjonalitet som i tillegg til manuelt valg, velger SBAS eller GBAS automatisk avhengig av hvilke signaler som er tilgjengelige og som gir den beste integriteten. Både GBAS- og SBAS-signalene gir integritetsalarmer for GPS. Ikke alle DGPS-mottakere har nødvendig funksjonalitet for å vise integritetsalarmene. Avhengig av type GPS-mottaker vil begrepene SBAS, WAAS eller DGPS benyttes om hverandre. GBAS benevnes i enkelte mottakere som «Beacon». Topografiske forhold i eksempelvis fjorder der signalveien går over høyt terreng kan medføre at DGPS-beregningene i mottakeren blir unøyaktige.

Ved tap av mange påfølgende meldinger, vil DGPS korreksjonene bli gradvis eldre med den følge at posisjonsnøyaktigheten gradvis blir dårligere. Til slutt vil mottakerutstyret gå over til "kun GPS modus" og ignorere DGPS korreksjonene

Forventet og erfart posisjonsnøyaktighet

De nevnte faktorene som alle påvirker posisjonsnøyaktigheten inngår i GPS-feilbudsjettet. Dette er en oversikt over hvor stor innvirkning de forskjellige faktorene har på mottakerens posisjonsløsning. Avhengig av hvor gammel læreboken man benytter er, eller hvilken side på internett man besøker, vil den oppgitte innvirkningen og dermed posisjonsnøyaktighet variere.

For Sjøforsvarets vedkommende har man i SNP-500, reglement for utøvelsen av navigasjon på Sjøforsvarets fartøyer, operert med absolutte verdier hentet fra foreldete versjoner av feilbudsjettet for å angi GPS posisjonsnøyaktighet. SNP-500 vil i løpet av 2018 komme i ny utgave og da være gjeldende for utøvelsen militær navigasjon på Forsvarets fartøyer.

I den nye utgaven av SNP-500 har man gått bort fra absolutte verdier og bruker i stedet forventet posisjonsnøyaktighet. Denne angis til å være mellom 3 og 10 meter 95 % av tiden både for sivil og militær GPS. For DGPS basert på åpne tjenester angis forventet nøyaktighet til mellom 1 og 3 meter 95 % av tiden. Disse verdiene er basert på den tidligere nevnte undersøkelsen av SPS posisjonsnøyaktighet.

Like viktig som forventet posisjonsnøyaktighet er den erfarte nøyaktigheten. Denne vil være avhengig av type GPS-antenne, hvilken høyde den har, type og fabrikat av GPS-mottaker samt operasjonsområde. Først når forventet nøyaktighet er avstemt med erfart, har man grunnlag for å kunne anvende GPS i høypresisjons militær navigasjon.

How does the civil maritime stand alone GPS user receiver computes its position?

Henning Sulen

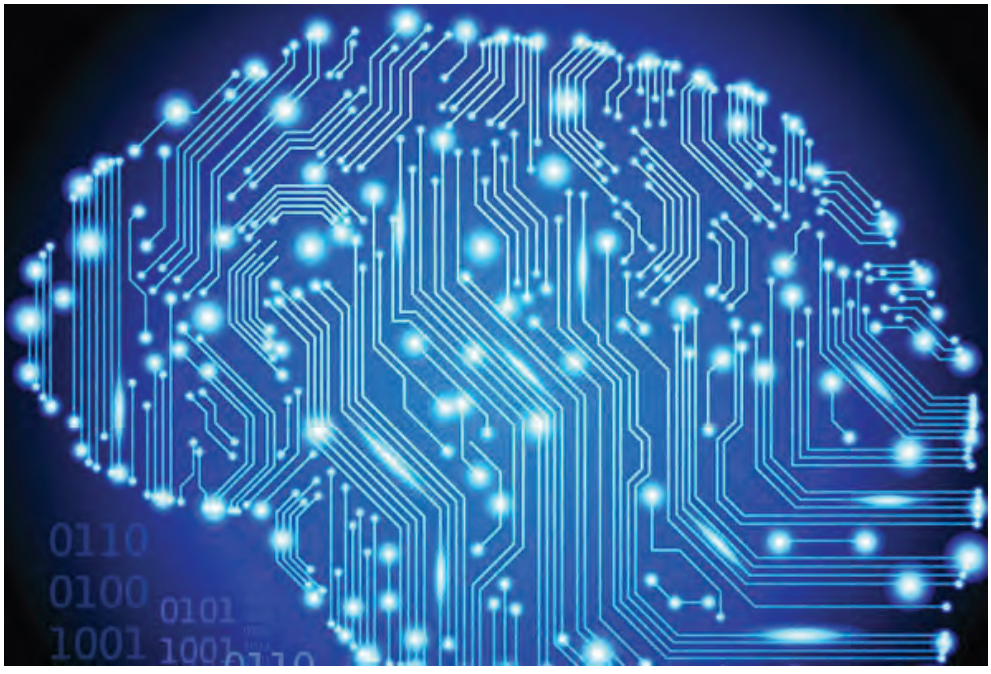


Figure: Esperanto 4k processor chip (eenewsanalog.com)

Navigation by Satellite Ranging and Timing (NAVSTAR) Global Positioning System, known simply as GPS has provided safe position and navigation for seafarers in decades. The civil maritime GPS receivers use the coded GPS satellite signals to compute its station position and with it give the vessel's position. This article looks into the process and equations the civil maritime GPS receiver uses to compute its position.

Global Navigational Satellite systems (GNSS) are the term for those navigation systems that provide the user with a 3-Dimentional positioning solution by passive ranging using radio signals transmitted by orbiting satellites (Groves 2013). In 1995 the Global Positioning System (GPS) became the first fully operational GNSS system with 24 satellites. GPS is developed, owned and operated by the USA, and is the most used maritime positioning system (GPS 2018).

According to the official U.S. government information about the GPS, the performance level of GPS Standard Positioning Service (SPS) Performance Standard for the GPS signal in space will provide a "worst case" pseudorange accuracy of 7.8 meters at a 95% confidence level (GPS 2018).

GPS coordinate system

GPS uses the Cartesian coordinate system with the three axis X, Y, Z. The directions synchronized to the Word Geodetic System 84 (WGS 84) which uses location of the Earth axis from South to North Pole in 1984 as reference (QPS 2018).

GPS Time

The GPS system is based on time. The GPS Time (GPST) was matched to Universal Coordinated Time (UTC) in 1980, and is today defined as UTC + 18 seconds (included the last leap second 1 January 2017) (QPS 2018).

Principle of civil maritime GPS stand alone pseudorange positioning

GPS is a one-way ranging system from the satellites to the users. Stand alone positioning is accomplished by use of the timing codes and the GPS satellite navigation message. The positions of a user station are computed using its observed pseudorange. The user receiver has four numbers of unknowns which are the Cartesian X, Y, Z and receiver clock offset. The receiver needs minimum four simultaneous pseudorange observations to four satellites to form four full pseudorange observed equations in the time frame of receiver (Bingley 2014).

Stand alone pseudorange observation equations

The term stand alone is used when the GPS receiver computes the position by itself.

Pseudorange is an "apparent range" between the satellite and the receiver that does not match with its geometric distance due to GPS bias and errors (ESA 2018).

Dr Bingley defines measure of range using pseudo-range as: *"A pseudorange is a direct measure of the one-way range (distance) from a satellite to a receiver, based on code (cross) correction of the incoming and replica signals to calculate the time-of-flight, and multiplying this by the speed of light"* (Bingley 2014).

The receiver receives incoming code signals using one channel per satellite unique code signal. It creates replica signals and uses code cross correlation of the incoming and replica signals to calculate the time-of-flight, assuming the satellite and receiver clocks are synchronized. The difference in time between the transmitted code from satellite and the replica code generated in receiver multiplied by the speed of light is the Pseudo-range. Pseudorange is corrupted by satellite clock offset, receiver clock offset, ionospheric- and tropospheric bias (Bingley 2014).

Figure: GPS satellite Block IIF (losangeles.af.mil)

The pseudo-range observation equation for stand-alone is (Bingley 2014)

$$PR^{S}_{r}(\tau_r) = \rho^{S}_{r}(T^{S}, T_r) + c\,[\,\delta\tau_r(\tau_r) - \delta t^{S}(t^{S})\,] + dion^{S}_{r} + dtrop^{S}_{r} + v^{S}_{r} \quad (1)$$

where

$PR^{S}_{r}(\tau_r)$ is the *pseudo-range* between satellite s and receiver r... in the *receiver time frame* τ of receiver r.

$\rho^{S}_{r}(T^{S}, T_r)$ is the *geometric range* between satellite s and receiver r... in the *true GPS time frame* T.

c speed of light in vacuo.

$\delta\tau_r(\tau_r)$ is the *receiver clock offset* for receiver r... in the *receiver time frame* of receiver r.

$\delta t^{S}(t^{S})$ is the *satellite clock offset* for satellite s... in the *satellite time frame* t of satellite s

$dion^{S}_{r}$ is the modelled bias due to ionospheric delay between satellite s and receiver r.

$dtrop^{S}_{r}$ is the modelled bias due to tropospheric delay between satellite s and receiver r.

v^{S}_{r} is the observation residual.

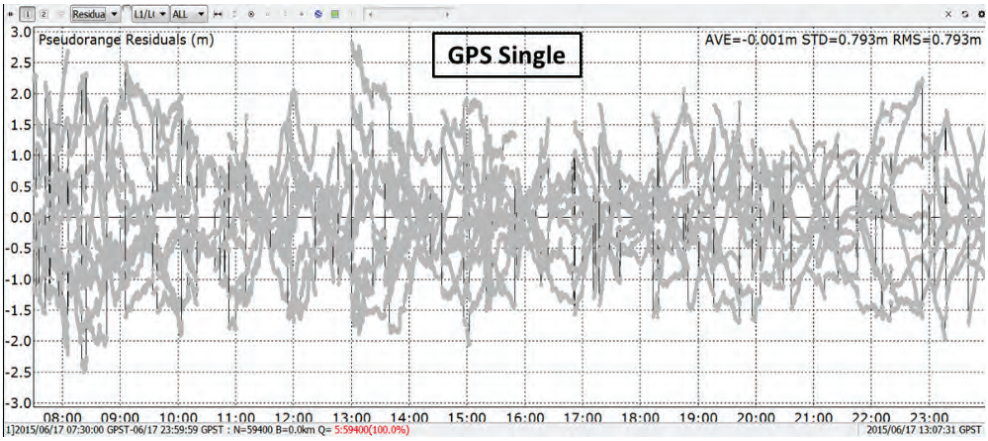


Figure: Plot of the GPS Single pseudorange residuals in times. X-axis is the GPS time and Y-axis is the residuals in meter. Pseudorange measurement residual is the difference between the expected measurement pseudorange and the observed pseudorange. The pseudorange residuals are the rest of systematic error and biases not counted for in the equations (Sulen 2015).

The three-dimensional coordinates of satellite s and receiver r are in the *Geometric range*, as…

$$\rho^{S}_{r} = \sqrt{[\,(X^{S} - X_{r})^2 + (Y^{S} - Y_{r})^2 + (Z^{S} - Z_{r})^2\,]} \qquad (2)$$

where

(X^{S}, Y^{S}, Z^{S}) are the Cartesian *coordinates* of satellite s...

(X_{r}, Y_{r}, Z_{r}) are the Cartesian *coordinates* of receiver r.

Least square implementation is used to solve the Cartesian coordinates of user receiver's four or more pseudo-range observation equations. Least square is a standard approach in regression analysis to the approximate solution where sets of equations are more equations than unknowns. "Least squares" means that the overall solution minimizes the sum of the squares of the errors made in the results of every single equation (Smith 2014).

The typical notation for the least squares observation equation is (Bingley 2014)

$$\mathbf{A} \cdot \mathbf{x} = \mathbf{b} + \mathbf{v} \qquad (3)$$

where

A is a matrix containing the coefficients of the observation equation.

x is a vector containing the corrections to the unknown parameters in the observation equation.

b is a vector containing the *observed-computed* values.

v is a vector containing the residuals.

Considering one receiver (a) and four satellites (e, n, o and v) a least square solution could be set up with the following A matrix and x, b and v vectors (Bingley 2014).

$$A = \begin{bmatrix} \frac{-(X^{e} - X_{a})}{\rho^{e}_{a}} & \frac{-(Y^{e} - Y_{a})}{\rho^{e}_{a}} & \frac{-(Z^{e} - Z_{a})}{\rho^{e}_{a}} & 1 \\ \frac{-(X^{n} - X_{a})}{\rho^{n}_{a}} & \frac{-(Y^{n} - Y_{a})}{\rho^{n}_{a}} & \frac{-(Z^{n} - Z_{a})}{\rho^{n}_{a}} & 1 \\ \frac{-(X^{o} - X_{a})}{\rho^{o}_{a}} & \frac{-(Y^{o} - Y_{a})}{\rho^{o}_{a}} & \frac{-(Z^{o} - Z_{a})}{\rho^{o}_{a}} & 1 \\ \frac{-(X^{v} - X_{a})}{\rho^{v}_{a}} & \frac{-(Y^{v} - Y_{a})}{\rho^{v}_{a}} & \frac{-(Z^{v} - Z_{a})}{\rho^{v}_{a}} & 1 \end{bmatrix} \qquad (4)$$

$$x = \begin{bmatrix} \Delta X_{a} \\ \Delta Y_{a} \\ \Delta Z_{a} \\ \Delta c\delta\tau_{a} \end{bmatrix} \qquad (5)$$

$$b = \begin{bmatrix} \text{observed PR}^{e}_{a} - (\rho^{e}_{a} + c.\delta\tau_{a} - c.\delta t^{e} + \text{dion}^{e}_{a} + \text{dtrop}^{e}_{a}) \\ \text{observed PR}^{n}_{a} - (\rho^{n}_{a} + c.\delta\tau_{a} - c.\delta t^{n} + \text{dion}^{n}_{a} + \text{dtrop}^{n}_{a}) \\ \text{observed PR}^{o}_{a} - (\rho^{o}_{a} + c.\delta\tau_{a} - c.\delta t^{o} + \text{dion}^{o}_{a} + \text{dtrop}^{o}_{a}) \\ \text{observed PR}^{v}_{a} - (\rho^{v}_{a} + c.\delta\tau_{a} - c.\delta t^{v} + \text{dion}^{v}_{a} + \text{dtrop}^{v}_{a}) \end{bmatrix} \qquad (6)$$

$$v = \begin{bmatrix} v^{e}_{a} \\ v^{n}_{a} \\ v^{o}_{a} \\ v^{v}_{a} \end{bmatrix} \qquad (7)$$

In general, least squares enable the x vector to be solved as (Bingley 2014)

$$\mathbf{x} = \mathbf{N}^{-1}\,\mathbf{d} \qquad (8)$$

where

$$\mathbf{N} = \mathbf{A}^{T}\,\mathbf{A} \text{ (or } \mathbf{A}^{T}\,\mathbf{P}_{l}\,\mathbf{A})$$
$$\mathbf{d} = \mathbf{A}^{T}\,\mathbf{b} \text{ (or } \mathbf{A}^{T}\,\mathbf{P}_{l}\,\mathbf{b})$$

and P1 are the a-priori weights of the equations, with the pseudorange typically either being given equal weights or being weighted with respect to elevation angle.
The process is repeated whereby a vector of unknown parameters (X) is created from the unknown parameters at the previous iteration (X*) and the x vector

$$\mathbf{X} = \mathbf{X}^{*} + \mathbf{x}\,. \qquad (9)$$

After the corrections in the x vector are considered negligible, an assessment of quality can then be obtained through the covariance matrix

$$\mathbf{C}_{x} = \mathbf{N}^{-1}\,. \qquad (10)$$

The full procedure employed by a receiver in a sequence of epochs would be as follows (Bingley 2014):

(i) For each satellite, calculate the satellite clock offset (in the satellite time frame) and the time of transmission (in the GPS time frame), from the information given in the broadcast ephemeris.
(ii) For each satellite, calculate the satellite coordinates at the time of transmission (in the GPS time frame), from the information given in the broadcast ephemeris, and then calculate the computed pseudorange,

based on the approximate station coordinates and the satellite coordinates.

(iii) Form the A matrix, b vector, N matrix, d and v vector, then solve for the x vector and update the approximate station coordinates.

In practice, steps (ii) and (iii) would then be repeated until the corrections to the approximate station coordinates are negligible.

The positions in X, Y and Z are converted into Latitude, Longitude and Height, and for maritime users normally transferred into the bridge system and Electronic Chart Display and Information System (ECDIS).

The levels of plan and height accuracy can be calculated by using Gauss propagation of errors law (Bingley 2014).

I.e.

$$\text{Accuracy} = \sqrt{(\text{satellite coordinate error})^2 + (\text{satellite clock error})^2 + (\text{ionosphere bias})^2 + (\text{troposphere bias})^2} \quad (11)$$

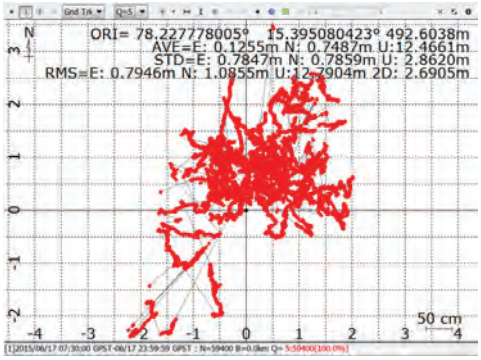


Figure: GPS plan scatter plot. Origin is the true position. Grid scale is 50 cm. The X-axis is West/East and Y-axis is North/South in meters. Due to changes in the GNSS systematic error and biases from epoch to epoch, the GPS epoch positions are also changed (Sulen 2018).

Summary

The article has provided an insight into how the GPS receiver uses the pseudorange equation, the least square-matrix and a-priori weights of the equations to compute the position. The receiver uses the result of last epoch as input to compute the next epoch position.

References

Bingley, R. (2014), Handouts Satellite Based Positioning (H24VST), The University of Nottingham, Nottingham, UK.

ESA (2018), GNSS *basic* [Online] Retrieved from: http://www.navipedia.net/index.php/GNSS_Basic_Observables on 27 May 2018

Groves, P. (2013), *GNSS, Inertial, and Multisensor Integrated Navigation Systems*. Boston, London, UK: Artech House.

GPS (2018), *GPS students* [Online] Retrieved from: http://www.gps.gov/students on 25 May 2018

GPS (2018), *GPS performance* [Online] Retrieved from: https://www.gps.gov/systems/gps/performance/accuracy/ on 25 May 2018

QPS (2018), QPS *wgs84* [Online] Retrieved from: https://confluence.qps.nl/qinsy/en/world-geodetic-system-1984-wgs84-29855173.html on 26 May 2018

QPS (2018), QPS *UTC to GPS time* [Online] Retrieved from: https://confluence.qps.nl/qinsy/en/utc-to-gps-time-correction-32245263.html on 26 May 2018

Smith, M. (2014), Lectures and Handouts in Least squares, The University of Nottingham, Nottingham, UK.

Sulen, H. (2015), *Civil Maritime GNSS Combinations in Arctic Areas.* MSc. Nottingham Geospatial Institute, The University of Nottingham, Nottingham, UK.

Navigasjonskrigføring (NAVWAR) med fokus på defensive tiltak

Øystein Glomsvoll

Sammendrag

Tilsiktet interferens (jamming) på GNSS-frekvensene er et vesentlig virkemiddel innenfor navigasjonskrigføring. Denne artikkelen beskriver elementer av defensive navigasjonskrigføringstiltak med fokus på hvordan en kan redusere påvirkningen fra jamming i mottakere og antennesystem samt bruk av alternative navigasjonsmetoder. Defensive NAVWAR-tiltak er viktig for opprettholdelse av kampkraft i Forsvaret, og vil bidra til å kunne opprettholde PNT-informasjon i NAVWAR-scenarier.

De siste årene har tilsiktet radiofrekvensinterferens (RFI) – jamming – mot signalene fra globale satellittnavigasjonssystemer (GNSS) blitt mer og mer utbredt, og sårbarheten til GNSS har fått en stadig større oppmerksomhet[1]. Vi har for eksempel hatt to dokumenterte hendelser med GPS-jamming fra Russland i Øst-Finnmark i september 2017 og mars 2018[2].

Primær kilde til posisjonsangivelse, navigasjon og tidsangivelse (PNT) i Forsvaret er det amerikanske NAVSTAR GPS. I tillegg finnes tre andre globale satellittnavigasjonssystemer, hvor kun det russiske GLONASS har nådd full konstellasjon. Det europeiske Galileo og det kinesiske BeiDou vil etter planen være oppe med full konstellasjon rundt 2020. Felles for alle GNSS er at svært lav effekt på signalene som mottas, samt bruken av faste og kjente frekvenser, gjør dem sårbare for både tilsiktet og utilsiktet interferens og følgelig begrenset eller ingen tilgang til PNT-informasjon.

Selv om denne sårbarheten er kjent, har Forsvaret gjort seg særdeles avhengig av PNT-informasjon fra GNSS. For eksempel er de fleste systemer på moderne marinefartøy avhengig av PNT-informasjon. Her inngår blant annet navigasjonssystemer, våpen- og sensorsystemer, kommunikasjonsutstyr og ubemannede systemer.

Samarbeid mellom Navkomp og FFI har tidligere resultert i gode erfaringer med å gjennomføre jammeprøver, både på NATO-øvelser og i nasjonal regi. I disse forsøkene har deteksjon og lokalisering av jammekildene vært en biaktivitet. I tillegg har FFI i de siste årene arbeidet med deteksjon av interferens på GPS-signalet hvor resultatene viser at GPS-jammere brukes av sivile, også i Norge[3].

NAVWAR

Navigasjonskrigføring, NAVWAR[4], er i NATO definert som militære operasjoner eller aktiviteter for å oppnå PNT overlegenhet. Disse militære operasjonene skal dermed sikre at egne enheter bibeholder PNT-informasjon samtidig som en hindrer tilgang for fiendtlige styrker. Operasjonene kan derfor karakteriseres som defensive og offensive, og denne artikkelen vil fokusere på de

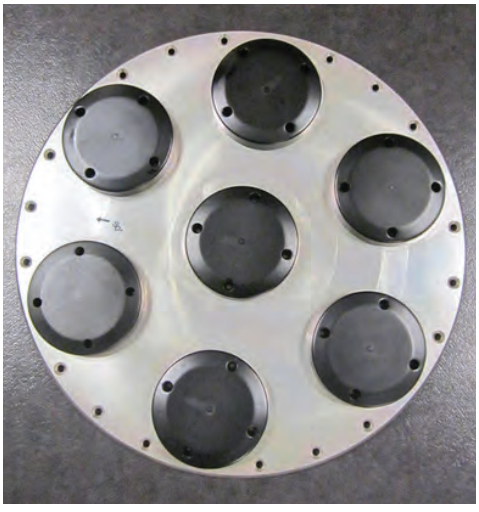
[1] *Norsk Romsenter (2013): «Vurdering av samfunnsmessig sårbarhet rundt bruk av globale satellittnavigasjonssystemer»*
[2] *www.aldrimer.no/ny-runde-med-gps-jamming-i-ost-finnmark/*
[3] *www.tu.no/artikler/her-passerer-flere-gps-jammere-hver-dag/232028*
[4] *Beskrevet i NATO STANAG 4621*

defensive NAVWAR-tiltakene. Sjøforsvarets strategiske konsept fastslår at *«defensive GNSS-tiltak for å opprettholde PNT-informasjon i et miljø der GNSS jamming skjer må prioriteres for opprettholdelse av kampkraft»*[5]. Defensive NAVWAR-tiltak handler om å beskytte egen PNT-informasjon når en utsettes for en jammetrussel. Disse tiltakene kan deles inn i tre hovedgrupper:

- Påvirkningen av jamming reduseres ved å gjøre GNSS-mottakere og antennesystemer mindre sårbare.
- Effekten av jamming reduseres ved å benytte alternative navigasjonsmetoder og alternative kilder til PNT (f.eks. terrengnavigasjon, treghetsnavigasjon og bruk av atomur).
- Inneha og bruke teknologi som gjør det mulig å detektere jamming på et tidlig tidspunkt, lokalisere jammekilden og varsle.

Redusere påvirkningen av jamming

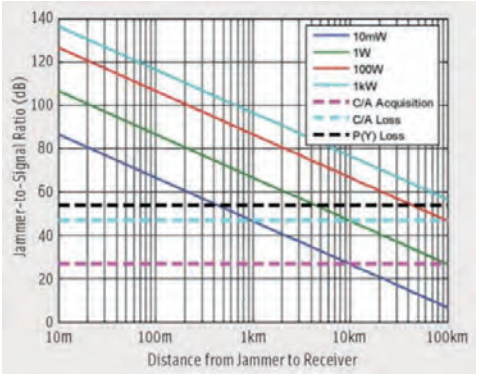
Påvirkningen fra jamming kan reduseres ved blant annet å utnytte flere GNSS (f. eks. Galileo i tillegg til GPS) samt oppgradere mottakere og antennesystem så ofte at man utnytter fordelene av den pågående teknologiske utviklingen. For militære brukere er det også viktig å benytte seg av robuste militære mottakere.



Figur 1. CRPA antenne med 7 elementer (kilde: http://gpsworld.com/anti-jam-protection-by-antenna/)

Tidligere forskning utført av Navkomp i samarbeid med Universitetet i Nottingham har funnet at bruk av multikonstellasjonsmottakere som kombinerer satellittsystemene GPS og GLONASS gir en økt robusthet mot jamming[6]. Siden fremtidige militære GNSS-mottakere mest sannsynligvis vil være multikonstellasjons mottakere som skal kunne kombinere signaler fra GPS og Galileo, bør en videre ha fokus på å studere utnyttelse av denne kombinasjonen for å redusere påvirkningen av jamming. Multi-GNSS mottakere vil dra fordeler av flere tilgjengelige signal og bedre geometri som også kan bidra til å forbedre nøyaktigheten.
Bruk av jammemotstandige antennesystemer som kan redusere antenneforsterkningen i retning mot en jammer har vist seg å være meget godt egnet i NAVWAR-scenarier (ref. FFI-rapport 17/16482 - NAVWAR during NATO Trial NEMO 2016). Disse antennesystemene kalles ofte nullstyringsantenner eller Controlled Reception Pattern Antenna (CRPA), og består vanligvis av syv elementer slik figuren under viser[7]. Resultater fra øvelser med tilsiktet interferens viser at bruk av slikt antennesystem gir en betydelig bedre robusthet mot jamming.

Militære mottakere har mulighet til å motta kryptert GPS-signal på to ulike frekvenser. Den krypterte P(Y)-koden er mer robust enn den sivile C/A-koden på grunn av blant annet krypteringsalgoritmen samt at de militære signalene har ti ganger større båndbredde enn de sivile signalene. Figuren under illustrer fordeler ved bruk av militær P(Y)-kode i forhold til sivil C/A-kode når det jammes med ulike efffekter (10mW – 1kW).



Figur 2. Effekten til ulike jammere på miltært (P(Y)) og sivilt (C/A) GPS-signal [8]

[5] *Sjøforsvarsstaben (2014): Sjøforsvarets strategiske konsept 2016 – 2040, Vedlegg D Teknologi*
[6] *Journal of Navigation (2017): «GNSS Jamming Resilience for Close to Shore Navigation in the Northern Sea*
[7] *http://gpsworld.com/anti-jam-protection-by-antenna/*
[8] *Jones, M. (2011): "The Civilian Battlefield. Protecting GNSS Receivers from Interference and Jamming" in InsideGNSS March/April 2011*

Som vi ser av figuren vil en jammer på 1W (grønn diagonal linje) kunne medføre at sivile C/A-kode mottakere mister signalet på en avstand til jammeren på 10 km mens tilsvarende for en militær P(Y)-kode mottaker vil være 4 km. En sivil mottaker vil ikke klare å starte «track» av signalet etter å ha mistet det før distansen til den samme jammeren er 100 km eller mer. Som vist over er bruk av multikonstellasjonsmottakere, militære mottakere og anti-jamme antennessytemer viktige defensive tiltak i NAVWAR-scenarier for opprettholdelse av PNT-informasjon når det jammes på GNSS-frekvensene.

Benytte alternative kilder til PNT

Når vi snakker om alternative PNT-kilder er det vesentlig at dette er reelle kilder som ikke benytter seg av satellittbasert teknologi og dermed vil være tilgjengelig når man er utenfor satellittdekning eller i områder med interferens. Alternative kilder kan deles inn i aktive og passive systemer avhengig om de krever utsendelse eller ikke, og militære enheter som forventes å operere i krise og krig bør i størst mulig grad basere seg på passiv navigasjon.
Innenfor alternative navigasjonssystemer skjer det en stor teknologisk utvikling. Den mest brukte alternative navigasjonskilden er treghetsnavigatorer koblet sammen med GNSS i et integrert navigasjonssystem. Ved bortfall av GNSS vil treghetsnavigasjon degraderes over tid, og et eksempel på ny teknologi som kan gi redundans er utnyttelse av gravitasjonsfelt for å forbedre navigasjonsnøyaktigheten (ref. FFI rapport 2016/026 – Feasibility study for gravity-aided navigation on the Norwegian shelf). Andre eksempler på alternative navigasjonskilder er terrengnavigasjon der f.eks. høyoppløselig bunndata kan benyttes for sjøgående enheter samt tradisjonell terrestriel navigasjon.
Alternativ kilde for tid kan være atomur som vil sikre en god nok back-up for tidskritiske systemer. Atomur i GNSS-mottakere vil også sørge for raskere GNSS-posisjonsløsning etter operasjon i områder uten tilgjengelige GNSS-signaler.
For å oppnå tilfredsstillende ytelse og redundans må fremtidige PNT-systemer inneha en integrert sammensetning av flere sensorer, og det er viktig at det integreres sensorer som ikke er avhengig av satellittbaserte systemer og kan fungere som et reelt alternativ til disse.

Deteksjon av jamming

Den tredje hovedgruppen av defensive navigasjonskrigføringstiltak omhandler deteksjon av tilsiktet interferens for å kunne gi en tidlig varsling for utsatte enheter. For Forsvaret er det viktig å inneha ESM-sensorer som er designet for å detektere og lokalisere jamming i GNSS-frekvensområdet.
Navkomp har tidligere beskrevet et konsept for deteksjon og varsling av jamming basert på informasjon Sjøforsvarets fartøy allerede har tilgjengelig, der det kan utvikles en algoritme for deteksjon og varsling av en jammetrussel. Deteksjonsalgoritmen som baseres på anvendelse av tilgjengelig informasjon i GNSS-mottakerene er tidligere beskrevet i Necesse[9] og «Pan European Networks – Government»[10] og er basert på signal-til-støy-forhold (SNR) fra hver enkelt satellitt som er tilgjengelig i brosystemene på fartøyene. SNR-informasjonen videresendes fra GNSS-mottakerne til brosystemene via NMEA[11]-protokollen, og ved å utnytte denne informasjonen vil en ha mulighet til tidlig deteksjon og varsling, noe som er essensielt for å iverksette andre tiltak innen navigasjonskrigføring.

Konklusjon

Tilsiktet interferens på GNSS-frekvensene er i de senere år blitt svært utbredt, og dette har blitt et viktig virkemiddel innenfor navigasjonskrigføring. Artikkelen har beskrevet elementer av defensive navigasjonskrigføringstiltak med fokus på hvordan en kan redusere påvirkningen fra jamming i mottakere og antennesystem samt bruk av alternative navigasjonsmetoder. Deteksjon av jamming er også vesentlig i et NAVWAR-scenario, og spesielt viktig er dette for kampsystemer som benytter ubemannede og autonome plattformer. Disse vil i høy grad være avhengig av GNSS-informasjon, og en tidlig deteksjon og varsling av en jammetrussel vil være nødvendig for sikker operasjon av slike plattformer.
Fokus på å inneha og iverksette defensive NAVWAR-tiltak vil bidra til å kunne opprettholde PNT-informasjon i NAVWAR-scenarier som videre sørger for opprettholdelse av kampkraft i Forsvaret.

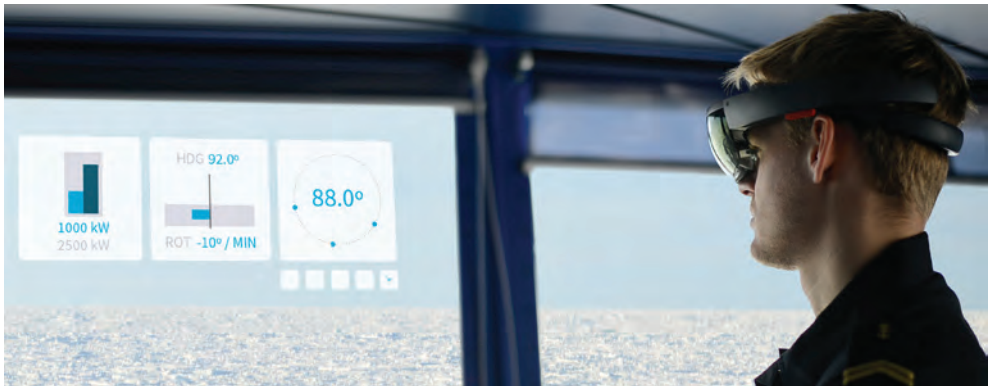
[9] *Necesse (2016): «GPS-jamming»*
[10] *www.paneuropeannetworkspublications.com/GOV20/#206*
[11] *The National Marine Electronics Association*

Feltstudier for design av utvidet virkelighets-teknologi i navigasjon

Synne G Frydenberg, PhD kandidat Arkitektur- og designhøgskolen i Oslo, Ocean Industries Concept Lab
Kjetil Nordby, Førsteamanuensis Arkitektur- og designhøgskolen i Oslo, Ocean Industries Concept Lab
Odd Sveinung Hareide, Fagleder Elektronisk Navigasjon, Sjøforsvarets Navigasjonskompetansesenter

Sammendrag

Maritim trafikk i Arktis øker. Derfor er det behov for å forbedre navigatørers situasjonsbevissthet i arktiske farvann. Arkitektur- og designhøgskolen i Oslo i samarbeid med Sjøkrigsskolen forsker på hvordan dette kan gjøres med briller som kan blande digital informasjon med det en navigatør ser ut av vinduet på skipsbroen. Som et ledd i arbeidet har vi vært med KV Svalbard på tokt i Arktis for å forstå navigatørens behov og utfordringer i praksis. Dette har gitt oss økt forståelse for hvordan vi kan utforme neste generasjons utstyr som må støtte navigatørenes situasjonsbevissthet under ekstreme forhold.



Bilde: Eksempel på grensesnitt ved bruk av AR (Layout: Synne Frydenberg)

Global oppvarming fører til at en stadig større andel av havet i Arktis blir farbart (1). Skipstrafikken i denne regionen øker derfor betydelig, og vi kan forvente at farvann som tidligere var utilgjengelig i det høye nord vil om kort tid være trafikkerte kommersielle skipsruter. Dette er ikke uproblematisk siden Arktis byr på omfattende operasjonelle utfordringer på grunn av røffe is, strøm og værforhold. Mangel på presis navigasjonsinformasjon, værmeldinger, isforhold, breddefeil og varierende GNSS posisjoneringsfeil kan føre til at mannskap med utilstrekkelig erfaring fra arktiske strøk har økt risiko for å gjøre feilvurderinger som potensielt sett kan få store konsekvenser. Analyser av skipsulykker generelt viser at så mye som 85% av ulykkene involverer menneskelige feil (2), og at manglende situasjonsbevissthet (*Situation Awareness - SA*) utgjør en umiddelbar årsak (3). Disse problemene kan ofte relateres til mangelen fokus på menneskesentrert design i utvikling av maritime arbeidsplasser.

Bilder: Arktiske forhold på feltstudier med KV Svalbard i Vestisen (Foto: Lasse Thomasgård)

EU-prosjektet SEDNA ("Safe maritime operations under extreme conditions: the Arctic case") skal forsøke å løse noen av sikkerhetsutfordringene knyttet til økt skipstrafikk i Arktis. Arkitektur- og Designhøgskolen i Oslo (AHO) gjennom Ocean Industries Concept Lab (OICL) (4), er en av 13 partnere i prosjektet. AHO har lenge forsket på nye typer brukergrensesnitt på skipsbroer (5,6). I SEDNA skal vi forske på hvordan vi kan skape et brukersentrert operasjonsmiljø på broen for isgående fartøy ved hjelp av briller utstyrt med utvidet virkelighets-teknologi (engelsk forkortelse AR etter *augmented reality*). AR-teknologi gjør det mulig å føye til informasjon over den virkelige verden – utover det vi klarer å oppfatte gjennom sansene. I dag er dette mest kjent gjennom mobile applikasjoner som legger informasjon over et live videobilde. Men AR kan også realiseres gjennom AR-briller som projiserer virtuelle lag, i form av både grafikk og lyd, i brukerens synsfelt. Det er disse systemene vi jobber med i SEDNA.

I høyrisikodomener, slik som i det maritime, er situasjonsbevissthet et sentralt aspekt for at menneskene som utfører sikkerhetskritiske oppgaver skal kunne ta riktige beslutninger. AR har blitt brukt til å styrke slik bevissthet i luftfarten i mange år gjennom head up displays montert i cockpiten (7). Det er sannsynlig at godt designede AR-applikasjoner som lar en navigatør bruke brosystemene samtidig som han/hun følger med på det som skjer utenfor, også kan forbedre navigatørers situasjonsbevissthet. AR kan redusere tiden navigatøren er nødt til å kikke ned (*head-down time*) på brosystemene (8) og redusere feiltolkning av informasjon ved å relatere det direkte til den fysiske verdenen. I praksis vil navigatører kunne bevege seg fritt på broen mens de i «har på seg» et brukergrensesnitt som lar dem se situasjonsrelevant informasjon.

Selv om AR teknologi potensielt kan være nyttig for navigatører, må slike systemer designes for brukerens

Bilde: Testing av AR-brillen Microsoft Hololens. (Foto: Rachel Troye)

Bilde: Feltstudier på KV Svalbard. (Foto: Rachel Troye)

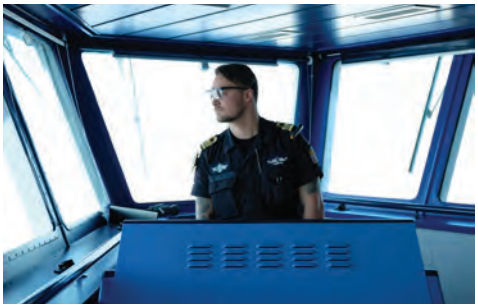
behov for å fungere i praksis. Per i dag er det få eksempler på *hvordan man skal designe* gode AR løsninger for maritimt personell. Derfor dreier AHO's forskning seg om hvordan vi kan designe bedre brosystemer støttet av slik AR-teknologi. Forskningen ligger innenfor praksisfeltet interaksjonsdesign. Interaksjonsdesign har som mål å skape muligheter for god interaksjon mellom mennesker og teknologi (9,10). Interaksjonsdesignere utarbeider grensesnitt for digitale produkter og tjenester slik at menneskene som bruker dem kan oppnå målene sine på best mulig måte.

For å legge til rette for god interaksjon, bør helst brukergrensesnittene relatere og tilpasse seg brukerens forventninger og erfaringer. Derfor er et sentralt aspekt i interaksjonsdesign å tilegne seg *brukerinnsikt; hvem er menneskene som skal bruke teknologien? Hva er deres mål? Hvordan løser de oppgaver? Hvilke prioriteringer gjør de? Hvorfor handler de som de gjør?* Svarene på disse spørsmålene påvirkes av situasjonene brukerne befinner seg i, og situasjonen er dermed et viktig aspekt i brukerinnsikten. For å designe fremtidens teknologiske løsninger kreves derfor omfattende innsikt i alle relevante forhold rundt situasjonene vi skal designe for, samtidig som vi utforsker teknologiske muligheter og premisser.

For å tilegne oss kunnskap om forutsetningene for bruk av AR i praksis, er det viktig å forstå eksisterende brukere i deres arbeidskontekst. Feltstudier er en viktig metode interaksjonsdesignere bruker for å få innsikt i situasjonen de designer for – både i praksis og ved forskning. Ved å tilbringe tid i det gitte miljøet, observere, snakke med brukere, kartlegge behov og teste ideer kan interaksjonsdesignere tilegne seg betydningsfull kompetanse (11). Fysisk og mental tilstedeværelse i en situasjon, gir oss som mennesker en helt annen type kunnskap som ikke kan oppnås på samme måte som ved å lese om den. Spesielt viktig og verdifull er denne kunnskapen når man skal designe for komplekse systemer innenfor høyrisikodomener, som for de fleste interaksjonsdesignere er et både ukjent og utilgjengelig felt.

Vi har nettopp gjennomført en slik feltstudie i SENDA prosjektet i samarbeid med Kystvakten. Da KV Svalbard skulle på fjorten dagers tokt til Vestisen sammen med Havforskningsinstituttet i mars, var vi tre medlemmer fra SEDNA-prosjektet på AHO som fikk en unik anledning til å delta for å gjøre et svært relevant feltstudium ombord. Hensikten med feltstudiet var å undersøke premisser og muligheter for utvikling av AR-systemer for navigasjon og operasjon i arktisk farvann. Samtidig var det viktig å bli kjent med arbeidssituasjonen på broen generelt, og spesielt under arktiske forhold. I tillegg til tradisjonelle forskningsmetoder som semistrukturerte intervjuer og deltakende observasjon, gjorde vi teknisk kartlegging av brokonsollene, test av AR-brillen Microsoft Hololens, test av dronefoto som tilleggsinformasjon for taktisk navigering i tett is og kartlegging av utvalgte scenarier, blant annet navigasjon i tett is. Ved hjelp av eyetracking-brillene Tobii Pro (12) samlet vi opptaksdata i flere seanser om hvor navigatøren til enhver tid hadde blikket under navigasjon i tett is fra brovingekonsollen. Denne type data viser hvor lenge og hvor ofte navigatøren ser på og veksler mellom ulike punkter foran seg, f.eks. ulike skjermer og isen som brytes rett foran baugen, og kan derfor fortelle oss mye om hvilken informasjon som til enhver tid er viktig for ham/henne å se ut i fra situasjonen(10).

Studien ga oss tilgang til en stor mengde data som vi bruker i utviklingen av AR demonstratorer. Foreløpig viser funnene fra feltstudien at plassering av informasjon og kontrollfunksjoner på broen slik den er utformet i dag, ikke er optimal for eksempel under navigasjon i tett is. I følge eyetracking-dataene, er navigatørene i testene avhengig av å følge svært nøye med på isens utforming i nær omkrets rundt baugen før og mens isen treffer, samtidig som de kontinuerlig trenger oppdatert informasjon om (kommer) fra brovingekonsollen. Dette betyr at navigatøren må hurtig og hyppig skifte fokus mellom disse to informasjonstypene ute i isen og inne på brovingekonsollen. Visuell og mental refokusering og reorientering mellom to områder med ulik avstand, tidvis svært ulik kontrast for øyet og kontinuerlig beregning av de ulike digitale og visuelle dataenes relasjon til hverandre, innebærer en betydelig kognitiv arbeidsbelastning for navigatøren. Mangel på nøkkelinformasjon som for eksempel motorkraft på brovingekonsollen gjør



Bilde: Innsamling av eye tracking data under navigasjon i tett is. (Foto: Rachel Troye)

i tillegg at navigatøren må forlate arbeidsstasjonen for å oppdatere seg på denne informasjonen ved hovedbrokonsollen. Ved bruk av AR-briller kunne hypotetisk sett den digitale informasjonen navigatøren til enhver tid har behov for vært plassert som et virtuelt lag oppå den reelle visuelle dataen navigatøren ser ut av vinduet. Når de ulike dataene ikke samsvarer kunne dette vært indikert og varslet for å øke navigatørens situasjonsbevissthet.

Vi ser også at dagens tradisjonelle brodesign har potensial for forbedring. Når kommende generasjoners grensesnitt for skipsbroer skal designes, må hele den fysiske utformingen tenkes gjennom på nytt. Kombinasjoner av gamle og nye grensesnitt og systemer byr på utfordringer f.eks. når det gjelder kontraster mellom ute og inne. Derimot kan operasjonsspesifikke situasjoner, slik som navigasjon i tett is, være verdt å vurdere å bruke AR-teknologi til. Spesialtilpassede AR-applikasjoner kan vise nøkkelinformasjon om fartøyets tilstand og om omgivelsenes tilstander projisert i navigatørens omgivelser. I tett is betyr dette for eksempel at navigatøren kan manøvrere fartøyet under krevende forhold uten å ta blikket vekk fra isen rundt baugen av fartøyet. Andre muligheter er å benytte AR-teknologi til å projisere data fra dronebilder av istilstander langs planlagt rute for at navigatøren lettere kan navigere taktisk med tanke på istykkelse og potensielle råk.

Feltstudien på KV Svalbard har vært svært viktig for prosjektet vårt og den har allerede ført til endringer og forbedringer i AR konseptene vi utviklinger i labben. I tiden som kommer vil vi utvikle nye demonstratorer som vi vil teste i kommende feltstudier. Samarbeidet med Sjøkrigsskolen og feltstudie på Sjøforsvarets fartøy har vært nyttig, og vi ser frem til videre samarbeid for å gjøre arbeidshverdagen til navigatøren enklere.

Kilder

1. Borgerson SG. Arctic Meltdown: The Economic and Security Implications of Global Warming. Foreign Aff. 2008;87(2):63–77.
2. McCafferty DB, Baker CC. Trending the causes of marine incidents. American Bureau of Shipping; 2006.
3. Procee S, Borst C, van Paassen MM, Mulder M. Toward Functional Augmented Reality in Marine Navigation: A Cognitive Work Analysis. 16th Conf Comput IT Appl Marit Ind [Internet]. 2017 [cited 2018 Apr 10]; Available from: http://resolver.tudelft.nl/uuid:67f92410-9e5a-452f-8fba-713f8d084cd2
4. Nordby K. Ocean Industry Concept Lab, Oslo School of Architecture and Design. Interactions. 2014;21(2):18–21.
5. Nordby K, Lurås S. Multimodal interaction for marine workplaces used as strategy to limit effect of situational impairment in demanding maritime operations. In 2015.
6. Nordby K, Morrison D. Designing calm technology and peripheral interaction for offshore service vessels - Semantic Scholar. Pers Ubiquitous Comput [Internet]. 2016 [cited 2017 Sep 23]; Available from: /paper/Designing-calm-technology-and-peripheral-interacti-Nordby-Morrison/102e6ed7f901729c40a684f9a9b6a7808af879e1
7. Melzer J, E Rash C. The Potential of an Interactive HMD Helmet-Mounted Displays: Sensation, Perception, and Cognition Issuses. In: Rash, Russo, Letowski, Schmeisser, editors. Helmet-Mounted Displays: Sensation, Perception, and Cognition Issuses. Fort Rucker, Alabama: US Army Aeromedical Research Laboratory; 2009.
8. Hareide OS, Ostnes R. Scan Pattern for the Maritime Navigator. TransNav Int J Mar Navig Saf Sea Transp [Internet]. 2017 Mar [cited 2018 May 14];11(1). Available from: https://trid.trb.org/view/1466779
9. Siang T. What is Interaction Design? [Internet]. The Interaction Design Foundation. 2018 [cited 2018 Apr 26]. Available from: https://www.interaction-design.org/literature/article/what-is-interaction-design
10. Buchanan R. Branzi's dilemma: design in contemporary culture. Des Issues. 1998;14(1).
11. Lurås S, Nordby K. Field studies informing ship's bridge design at the ocean industries concept lab. [Internet]. 2014 [cited 2017 Sep 21]. Available from: https://brage.bibsys.no/xmlui/handle/11250/221073
12. Tobii Pro Glasses 2 wearable eye tracker [Internet]. 2015 [cited 2018 May 14]. Available from: https://www.tobiipro.com/product-listing/tobii-pro-glasses-2/
13. Hareide OS, Ostnes R. Maritime Usability Study by Analysing Eye Tracking Data. J Navig. 2017 Sep;70(5):927–43.

For mer detaljert rapport anbefales rapporten etter forskningstoktet med KV Svalbard fra AHO. Rapporten blir fremsendt på forespørsel ved å kontakte Odd Sveinung Hareide (oddsveinung.hareide@sksk.mil.no)

NATOs tverrfaglige fokus på bruk av syntetiske miljøer for utvikling av nye kapabiliteter

Frode Voll Mjelde

Sammendrag

Forskning og utvikling innen anvendelse av syntetiske miljøer for å fremme krigføringskapasiteter i NATO har ofte har vært drevet av frittstående arbeid innen enkelte paneler og arbeidsgrupper, uten fokus på felles anvendelse. NATO har derfor valgt å sammenfatte aktiviteter innen simulering og trening til en gruppe som skal fokusere på tverrfaglig utnyttelse av simuleringskapabiliteter. I den forbindelse er NATO AWACS valgt for å demonstrere hvordan tverrfaglig utnyttelse av syntetiske miljøer kan øke NATOs kampkraft. Denne teksten informerer om dette arbeidet, og oppfordrer samtidig det norske Forsvar til å vurdere tilsvarende tiltak.

Nøkkelord: Militære anskaffelser, Koordinering mellom miljøer, Oppdragseffektivitet, Prestasjonsvurdering, Simulering, Syntetiske Miljøer, Systems Engineering, Test & Evaluering, Trening & Øving, NATO AWACS

I NATO er forskning og utvikling (FoU) beskrevet som nøye utvalgte og grundige prosesser som gir validert kunnskap for å kunne utvikle og anvende systemer og konsepter med høy ytelse for forsvars- og sikkerhetsformål. The Science and Technology Organization (STO) er en del av NATO strukturen, og har som formål å hente ut det beste av forskning og teknologi som hvert enkelt medlemsland kan tilby for å møte NATOs kollektive behov (NATO STO, 2018).

NATO STO ønsker økt anvendelse av sofistikerte modelleringer og simuleringsteknologier som kan vurdere nye kapabiliteters effektivitet. Høyt modenhetsnivå på simuleringsteknologier gjør det mulig å møte krav til kosteffektiv utnyttelse av teknologi for å skape mest mulig kampkraft for alliansen (NATO STO HFM, 2018).

NATO tverrfaglig arbeidsgruppe innen syntetiske miljøer

FoU innen syntetiske miljøer har ofte har vært drevet av spesifikke behov, uten en tilnærming til felles anvendelse av teknologi og forskningsmetode. NATO STO har derfor valgt å sammenfatte enkelte M&S aktiviteter til tverrfaglig utnyttelse av simuleringskapabiliteter i en arbeidsgruppe under HFM 268 - *Synthetic Environments for Mission Effectiveness Assessment*. Norge deltar i denne gruppen med representant fra NAVKOMP på vegne av Sjef Forsvarets Sanitet (SJ FSAN).

Formålet til HFM[1] 268 er å skape realistiske og kosteffektive syntetiske miljøer som muliggjør design og evaluering av nye alternative militære systemer, og å utvikle

[1] *HFM – Human Factors and Medicine*

effektive menneske-system kapabiliteter som opprettholder alliansens responskapasiteter. HFM 268 fokuserer derfor på syntetiske miljøer som integrerer «*human in the loop*» med simulerte operasjonsmiljøer.

Spesifikke mål for HFM 268 er definert som:

1. Identifisere troverdige måleparametre som kan vurdere og forutsi oppdragseffektivitet.
2. Identifisere utvikling av M&S-teknologi som møter fremtidige oppdragsbehov.
3. Utforske sivile simuleringer som kan tilpasses for militære applikasjoner
4. Identifisere applikasjonsmuligheter knyttet til trening og systemutvikling.
5. Oppsummere utfordringer innen menneske-maskin systemer og anbefale retningslinjer som støtter effektive design.
6. Identifisere teknologiske muligheter for aktive samarbeid innen alliansen og utvikle et strategisk veikart for anvendelse av syntetiske miljøer.

NATO Airborne Warning and Control System (AWACS)

HFM RTG-268 har valgt å fokusere på oppdrag som utføres av NATO Airborne Warning and Control System (AWACS) for å demonstrere innsamling av oppdragsrelevante beregninger og målbare ytelsesparametre i et syntetisk miljø. I tillegg skal arbeidsgruppen undersøke hvordan dette miljøet kan nyttes til objektiv evaluering av alternative luftbårne varslingssystemer og operasjonskonsepter.

NATO er interessert i å vurdere alternative metoder til luftbåren kommando og kontroll for varsling og koordinering i luftrommet. Nærmere bestemt; å overføre funksjoner som vanligvis utføres av AWACS til mindre fly og bakkestasjoner. Virkninger av en slik endring er imidlertid ikke fullt ut forstått, og det er behov for synliggjøring av muligheter og konsekvenser ved en slik endring. Den foreslåtte studien vil derfor sammenligne og evaluere dagens operasjoner med et mulig sammensatt luft-, og bakkebasert system for kommando kontroll i luftrommet. For å gjennomføre en slik aktivitet er det utviklet et utfordrende AWACS-oppdrag som skal analyseres i et realistisk syntetisk miljø. Målinger skal dekke ytelsen til både plattformen og mannskapet; herunder teknisk, taktisk og CRM[2] ytelse. Innsamlet data skal danne en baseline som i fremtiden skal nyttes for å evaluere oppdragseffekten av ny CONOPS sammenlignet med eksisterende CONOPS.

Warrior Preparation Center (WPC) i Tyskland er valgt for gjennomføring av studien, sammen med et virtuelt treningsmiljø tilknyttet NATO AWACS-skvadronen i Geilenkirchen, Tyskland. NAVAIRs Next Generation Threat System (NGTS) benyttes i den kvartalsvise Spartan Warrior-øvelsen til å introdusere nåværende og fremtidige militære kapabiliteter i et syntetisk miljø(Olde, 2017). WPC vil etter hvert installere Performance Evaluation & Tracking System (PETS) benyttet av Air Force Research Lab (AFRL) som skal samle automatiske ytelsesmålinger på operativ effekt, samt på teknisk og taktisk utførelse hos AWACS mannskap.

Deltakere fra HFM 268 har i løpet av 2017 og 2018 deltatt på øvelse Spartan Warrior for å etablere realistiske parametre for objektiv måling av ytelse på enhet

Figur 1, E-3A NATO 1 Squadron Tiger Jet (Foto: www.natotigers.org)

Mission statement nato airborne early warning and control force

"DELIVER READY, RESPONSIVE AIRBORNE EARLY WARNING, BATTLE MANAGEMENT AND COMMAND AND CONTROL CAPABILITY TO OPERATIONAL COMMANDERS IN SUPPORT OF NAC-APPROVED TASKINGS"

[2] *CRM – Crew Resource Management*
[3] *LVC – Live Virtual and Constructive*

Figur 2, NATO AWACS E-3A Component Logo

og mannskap. *Spartan Warrior Exercise* er en 4-dagers LVC[3] øvelse som dekker 1) Offensive Counter Air (OCA), 2) Defensive Counter Air (DCA), 3) Interdiction (INT), og 4) Close Air Support (CAS)/Strike. I tillegg inneholdt øvelsen Elektronisk krigføring (EW), Combat Search and Rescue (CSAR), og Airborne Alert Interdiction (XINT). NATO AWACS-mannskap deltok i arrangementer over alle fire dagene øvelsen pågikk. Scenariet fulgte et script basert på *Joint Master Scenario Event List* (JMSL), ut-arbeidet etter retningslinjer fra NATO AWACS trenings-mål. En ny JMESL er etablert for hver dag i øvelsen (tabell 1).

Tabell 1 viser de overordnete hendelsene for dagen, hvorpå en mer detaljert utgave vil beskrive hvilken enhet/spiller som er ansvarlig for å starte en begivenhet, tidspunktet for start og slutt, og det forventede resultatet av hver enkelt hendelse.

Basert på observasjoner av øvelsen i februar/mars 2018 identifiserte teamet enkelte mulige målinger som kan automatiseres: 1) Kontaktidentifikasjon, 2) Oppdragsansvar, 3) Allokering av ressurser og 4) Arbeidsbelastning (som vil kreve fysiologisk måling for å automatisere). Kandidater for subjektive og observatørbaserte tiltak inkluderer: 1) Crew Resource Management (CRM) ferdigheter, 2) Arbeidsbelastning, og 3) Kommunikasjon. Arbeidsbelastning kan måles automatisk og subjektivt. Tabell 2 viser et eksempel på hvordan dette kan gjøres i et syntetisk miljø.

HFM-RTG-268 har så langt fungert i en utforskende fase hvor en rekke observasjoner og rapporter av syntetiske og reelle NATO AWACS operasjoner er samlet inn. Det videre arbeidet vil fokusere på sammenfatning av disse dataene for å etablere grunnverdier (baseline) for objektive og subjektive ytelsesmål. Sammenfatningen vil resultere i forbedret utnyttelse av simuleringskapabilitet som en naturlig del av styrkeproduksjonen og uttesting av nye kapabiliteter som vil bidra til NATOs evne til å håndtere eksisterende og fremtidige utfordringer.

Tabell 1, Utdrag fra overordnet JMESL (Day 1)

Day 1

DAY 1 Vul Time1200-1430Z			
Major Planned Event - Strike Package SWA1 OCA Event			
Event	Time frame	Event	Outcome
1	1200 - 1230	Su-24 fly along border	AWACS tasks DCA to shadow
2	1200 - 1240	Strike Package SW1 requires additional assets, Grizzly 36 engaged by SA-11, Bails out in friendly territory	AWACS coords additional assets, On scene commander check list initiated
3	1255 - 1320	Defector profile, SAM's active, Mig-29 and Su-27 chase, Patriot handover	AWACS coords with AOC
4	1306-1400	DT Tasking for Pawnee 11 -Smack Grizzly 36 target, Investigate missile launchers	AWACS coords with AOC
5	1335 - 1400	HFF profile - Scram possibility	AWACS calls SCRAM
6	1350 - 1410	Red OCA package - 2 Su-24 (Fire cruise weapons) / 2Mig-29 (handled by Patriots) / 4 Su-27	Patriot Handoff
7	1400 -end	Tanker issues	AWACS coordinates

Tabell 2, Eksempel på automatisk eller observatørbasert måling av besetningens arbeidsbelastning

Performance Category	Measurement Type	Performance Measures	Implementation Considerations
Workload	Objective, outcome-based	• Physical workload	• Physiological measures (e.g., heart rate, galvanic skin response)
	Subjective, trainee-ratings; Subjective, observer-based	• Physical workload • Cognitive workload	• Assessment tools that have undergone psychometric validation available (e.g., NASA TLX)

Norsk utnyttelse av arbeidet i HFM-RTG-268

Forsvarets bruk av simulert støtte til utdanning og trening fungerer allerede som en kosteffektiv utnyttelse av teknologi for å skape mest mulig kampkraft, fra utdanning av individ til trening av team (Mjelde, 2013). Sjøforsvaret, Luftforsvaret, Hæren og HV innehar hver for seg kosteffektive simulatorsystemer anskaffet for behovsprøvd utdanning, trening og øving; innenfor hver forsvarsgren, innenfor spesifikke behov. I likhet med NATO STO oppnår vi gode resultater – men vi gjør det hver for oss; gren for gren, avdeling for avdeling. Det norske Forsvar bør, som NATO STO, ta initiativ til tverrfaglig og helhetlig tilnærming til en felles metode for ytelsesmålinger i syntetiske miljøer. Økt utnyttelse av Forsvarets simuleringskapabilitet således kunne gi et *positivt bidrag til alle Forsvarets oppgaver* (Forsvarsdepartementet, 2012), og kan gi Forsvarets ledelse forbedret SA om operative enheters egnethet i reelle miljøer, nasjonalt og internasjonalt.

Referanser

Forsvarsdepartementet. (2012). *Stortingsproposisjon 73 S - Et forsvar for vår tid.* Oslo: Det Kongelige Forsvarsdepartementet.

Mjelde, F. V. (2013). *Performance assessment of military teams in simulator and live exercises*. U.S. Naval Postgraduate School , Human Systems Integration. Monterey, CA: U.S. Naval Postgraduate School .

NATO STO. (2018, May 20). *about NATO STO*. Retrieved from NATO Science and Technology Organization: https://www.sto.nato.int/Pages/organization.aspx

NATO STO HFM. (2018, May 20). *Cross Panel Activity on Synthetic Environments for Mission Effectiveness Assessment.* Retrieved from https://www.sto.nato.int/search/Pages/activities_results.aspx?k=hfm%20268&s=Search%20Activities

Olde, B. (2017). *Commander*. Office of Naval Research (ONR).

DEL 4

Bacheloroppgaver
OM3 2018

Bacheloroppgaver 2018, operativ marine

Innlevering 29. mai 2018

Siste års kadetter ved operativ marine gjennomfører emne PP3051 Bacheloroppgave hvert vårsemester. Dette emnet innebærer 270 studietimer. Bacheloroppgaven skal gi kadettene anledning til å anvende kunnskaper og ferdigheter de har tilegnet seg ved bransjeutdanningen ved Sjøkrigsskolen. Oppgaven skal gi erfaring i å arbeide med en problemorientert oppgave, og den skal gi øvelse i å gjennomføre et større arbeid alene eller i gruppe. Den skal gi kadetten tid til fordypning og trening i å løse teoretiske, eksperimentelle eller praktiske problemstillinger.

Sjøforsvarets Navigasjonskompetansesenter har de siste årene hatt fokus på å styrke arbeidet med bacheloroppgaven, som et ledd i rettet forsknings- og utviklingsarbeid (FoU). Det er ønskelig at bacheloroppgaven skal besvare en relevant operativ problemstilling, som både kadetten og (Sjø)Forsvaret for øvrig skal ha nytte av. Operative avdelinger oppmuntres til å ta kontakt med Navkomp for å melde inn relevante problemstillinger til bacheloroppgaven.

Utvalgte ugraderte bacheloroppgaver vil bli gjort offentlig tilgjengelig via Bibsys Brages[1].

Oppgavene for 2018 vil bli presentert med postere på Navigasjonskonferansen på Sjøkrigsskolen 4-6. desember, og overskriftene er som følger:

[1] *https://brage.bibsys.no/xmlui/handle/11250/2382908*

1. *Stressaktivering – sammenlikning mellom virtuell og reell seilas*
Denne oppgaven måler aktivering av elektrodermisk aktivitet (EDA) hos navigatøren under seilas med skolefartøy og i simulator. Hensikten med oppgaven er å koble forskjeller/likheter i stressaktivering i de to domenene opp mot læringseffekter.

2. *Utarbeiding av undersøkelsesrapporter etter ulykke i Sjøforsvaret*
Hensikten med oppgaven er å vurdere hvordan en fast metodisk tilnærming (DoD HFACS) til undersøkelsesrapporter kan danne grunnlag for å avdekke og synliggjøre menneskelige faktorer ved ulykke.

3. *Brukervennligheten til Relative Terresterial System*
Relative Terresterial System (Terrest) er en valgbar posisjonskilde i navigasjonssystemet om bord på flere av Sjøforsvarets fartøy. Terrest baserer sin posisjonsberegning på terrestriske målinger fra ulike sensorer og er ikke avhengig av satellittbaserte navigasjonssensorer for å gi en posisjonsløsning. Oppgaven søker å forbedre brukervennligheten til Terrest.

4. *Remote Operator Centre (fjernstyringssentral) for operativ bruk i Sjøforsvaret*
Oppgaven vil være rettet mot utformingen av Sjøforsvarets ROC i fremtiden. Vi ønsker å spisse oppgaven mot noe mer spesifikt, men dog med hensyn til at dette er et felt som er i forskningsstadiet. Videre vil dette vinkles mot effektiv navigasjon for å kunne bidra til økt operativ nytte ved bruk i Sjøforsvaret.

5. *Navigatøren etter Sjøkrigsskolen - Prestasjon ved degradert GNSS*
Problemstillingen er: Er tredjeklasse kadetter ved operativ marine i stand til å oppdage en gradvis degradering av GNSS under oppdragsløsning? Det er tatt utgangspunkt i følgende hypotese: «Navigatøren vil støtte seg på systemene, herunder GNSS i stor grad og ikke legge merke til avvik før han/hun har avveket relativt sett mye fra faktisk posisjon.»

6. *Landobjekter som bør tilføyes i elektroniske navigasjonskart*
Vi opplevder på seilaser med skolefartøyene til Sjøkrigsskolen at det finnes objekter i området rundt Bergen som er egnet seg til bruk i navigasjon, men som ikke er å finne i de elektroniske navigasjonskartene. For å gjøre planleggingsarbeidet før seilas enklere hadde det vært en fordel om objekter som dette ble vist i de elektroniske navigasjonskartene. Er dette mulig?

7. *Militær presisjon i posisjon–En undersøkelse av ulike peilesøyler*
Sjøforsvarets fartøyer benytter seg av GPS og andre sensorer for å opprettholde sin posisjon i det elektroniske sjøkartet. Marinens fartøyer er også avhengige av å kunne skaffe seg en posisjon uten å ha signaler fra GPS. En av metodene fartøyene kan bruke er å bruke en peilesøyle for finne en posisjon med 2 eller 3 peilinger. Oppgaven tar for seg Sjøforsvarets 2 ulike peilesøyler og hvilken av disse som kan tilby et best mulig resultat. Problemstilling: Hvilken av peilesøylene vil gi best målinger ved posisjonering?

8. *Fartøysklarering ved hjelp av radar*
Under nedsatt sikt er det normalt for fartøyer å bruke radar for å unngå å komme nær eller unngå å kollidere med et annet fartøy. Forfatterne har gjennomført et forsøk i navigasjonssimulatoren der radaren er benyttet til å klarere fartøyer. Oppgaven tar for seg hvilke metoder et utvalg kadetter benytter til fartøysklarering i kontrollmoden radar.

9. *Kadettenes veivalg*
Problemstilling: Hva påvirker kadettenes veivalg ift videre tjeneste? Valg av tjenestested etter endt Sjøkrigsskole oppleves for noen som et sikkert og gjennomtenkt valg, mens for andre fremstår det som noe mer ukjent. Har kadettene tilstrekkelig kunnskap om de ulike våpen og plattformer før de skal velge tjenestested? Blir man påvirket av medieoppslag, av relasjoner til andre offiserer og kadetter, av forslag og oppfatning fra lokal veileder ved SKSK?

10. *Maritim etterretning*
Gradert oppgave

11. *Maritime Cyber Security (MCS)*
Problemstilling: Hvilken holdning til Maritime Cyber Security har dagens kadetter ved Sjøkrigsskolen, og samsvarer den med de krav som stilles til rutiner og datasikkerhet i Marinen?

DEL 5

Gjengivelse av artikler publisert
i andre tidsskrift

Improving Passage Information Management for the Modern Navigator

Odd Sveinung Hareide

Artiklen presenterer Sjøforsvarets Navigasjonskompetansesenter sin filosofi for gjennomføring av elektronisk navigasjon. Dette omhandler faser i navigasjon, og hvordan de er integrert i kommunikasjonsprosedyrene. Videre ser artikkelen på hvordan informasjonshåndteringen kan se ut i fremtiden.

Artikkelen ble levert og publisert i forbindelse med 19th IALA Conference 2018. International Association of Lighthouse Authorities (IALA) sin målsetning er å bidra til effektive og harmoniserte navigasjonshjelpemidler over hele verden. Implisitt hvordan de benyttes av sjøfarende.

Improving Passage Information Management for the Modern Navigator

Odd Sveinung Hareide

Royal Norwegian Naval Academy, Navigation Competence Centre

Bergen, Norway

SUMMARY

The main objective of the navigation system on board a vessel is contributing to safe operation, which is supported by a high degree of situation awareness for the navigator, in order to achieve a safe and efficient passage. On the modern bridge, an increasing amount of displays and support systems has been introduced, with computers being networked and integrated information presented on Multi-Function Displays. Presentation of relevant information for the navigator is crucial to reduce Head Down Time (HDT). The route monitor information relevance increases with challenging waters and higher speeds.

This paper presents a standard operating procedure on the planning and execution of a voyage, which is aligned with the Graphical User Interface (GUI) on the Electronic Chart Display and Information System (ECDIS) on board the vessel. This reduces workload and decrease HDT for the navigator. The paper further suggests the use of Augmented Reality (AR) in the future to continue the strive to reduce HDT and ease the burden for the maritime navigator.

RESUME

L'objectif principal du système de navigation à bord d'un navire est de contribuer à un fonctionnement sûr, qui s'appuie sur un degré élevé de conscience de la situation pour le navigateur, afin de parvenir à un passage sûr et efficace. Sur la passerelle moderne, une quantité croissante d'écrans et de systèmes d'aide a été introduite, avec des ordinateurs mis en réseau et des informations intégrées présentées sur des écrans multifonctions. La présentation des informations pertinentes pour le navigateur est cruciale pour réduire le temps de réflexion. La pertinence de l'information de suivi de la route augmente avec la difficulté de la mer et la vitesse.

Cet article présente une procédure opératoire standard pour la planification et l'exécution d'un voyage, qui est alignée avec l'interface utilisateur graphique (GUI) sur le système d'affichage et d'information des cartes électroniques (ECDIS) à bord du navire. Cela réduit la charge de travail et diminue le temps de réflexion pour le navigateur. Le document suggère en outre l'utilisation de la Réalité Augmentée (RA) à l'avenir pour poursuivre les efforts visant à réduire le temps de réflexion et alléger le fardeau pour le navigateur maritime.

CONTENTS

1. INTRODUCTION

Technology with the purpose to ease the burden for the navigator are being introduced on ship bridges. Electronic navigation has many useful tools, but should incorporate and facilitate for traditional principles of navigation to ensure a safe passage. Young navigators must have an extensive system knowledge together with traditional navigation skills, and learn not to put their whole trust in the information presented on the computer screen.

In maritime navigation, the navigator`s situational awareness (SA) is crucial to enhance the safe navigation and passage of the vessel (Hareide and Ostnes, 2017b). Information management on a modern maritime navigation system is provided on a multi-function display (MFD), with electronic chart system (ECS) or Electronic Chart Display and Information System (ECDIS). One important feature is to facilitate route monitoring in order to provide timely and relevant information presentation for the navigator.

To conduct a safe passage, the navigator plans the route carefully in advance. The route is planned using traditional navigation craftsmanship, which includes using heading points and turning points. The complexity of the planning and conduct of the passage varies with the spatial environment, such as above- and underwater topography, weather and the amount of aids to navigation in the fairway. The speed also contributes to added complexity, and the dynamics of the motion of the vessel will influence the navigator`s working environment.

Research has shown that the route monitoring Graphical User Interface (GUI) is not optimized, and that the use of MFDs induce Head Down Time (HDT) for the navigator. Figure 1 shows the scan pattern for the navigator on board a high speed craft (HSC), and is collected with the use of Eye Tracking Glasses (Hareide and Ostnes, 2017a).

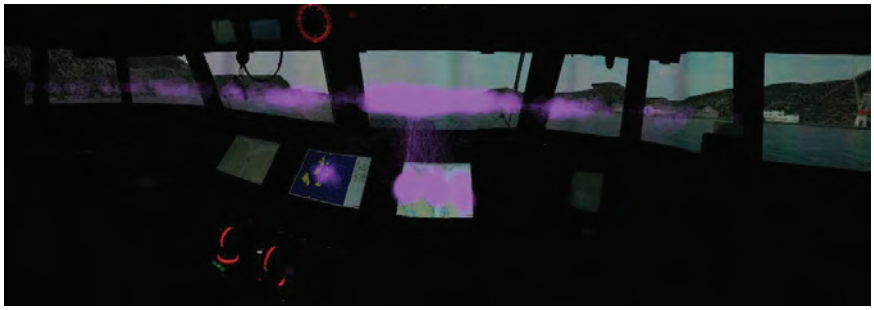


Figure 1: Scan path for a HSC Navigator

As the scan pattern reveals, the main focus of the navigator is towards the surroundings of the vessel, but also towards the navigation system information presented on MFDs. The visual view of the navigator is divided into Areas of Interest (AOIs), which in Figure 1 is divided into:

- AOI Outside: Consisting of the surroundings of the vessel, limited by the windows at the bridge.
- AOI ECDIS: The Electronic Chart Display and Information System presented on an MFD, in Figure 1 on the right side MFD.
    - AOI Route Monitor window is a part of the ECDIS GUI, which presents information related to the planned and monitored route.
- AOI Radar: The radar picture presented on an MFD, in Figure 1 the centre MFD.

The amount of time in different AOIs is shown in Figure 2, and one could argue that the navigator should address most of the time to the outside of the vessel, controlling and comparing the position

of the vessel towards the navigation system (Norris, 2010, Hareide and Ostnes, 2017b). The amount of time in the different AOIs is dependent on several factors, among others the environmental conditions and light conditions.

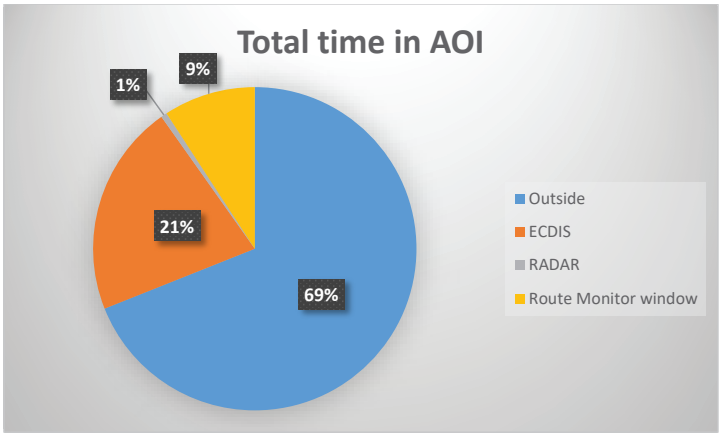


Figure 2: Total time in Areas of Interest (REFERANCE)

When conducting a passage in confined waters, continuous control of the surroundings of the vessel is essential. This implies that the amount of HDT should be minimized in order to facilitate safe navigation and cross-correlation of the vessels actual position compared to the position in the navigation system. New ways of presenting the relevant information for the maritime navigator could be beneficial, and augmented reality shows a good potential. However, the maritime industry is known to be a conservative industry, and new technology takes time do adopt to the maritime domain.

2. INFORMATION MANAGEMENT FOR THE MARITIME NAVIGATOR

2.1. TRADITIONAL SKILLS AND SYSTEM AWARENESS

Being a navigator on a modern ship today means working in a technologically advanced environment, which demands both a comprehensive understanding of systems as well as good navigation skills. When using an integrated and networked navigation system, there are several possible sources of error which may lead to errors in how the positioning is visually displayed. This means that continuous checks of the system are necessary. This may be done by traditional visual methods like taking cross bearings, or using other sensors like for instance radar.

In littoral waters there are multiple obstacles making navigation challenging, and when introducing increased speed, the amount of time for decision making reduces. In a littoral passage each leg will vary in length, but as an example, a leg of one nautical mile, which equals 1852 meters, will take two minute to complete in 30 knots. In demanding littoral waters, consecutive legs are often less than 0,5 nm in distance, making the decision process before the next leg less than one minute.

The navigation team needs to focus their attention towards the demanding task of conducting the safe and efficient passage, and it is thus imperative that there are no disturbing factors stealing the attention of the navigation team (Hareide et al., 2016).

The conduct of a safe passage is a complex task, conducted in a sociotechnical system as a navigation team (da Conceição et al., 2017). To support safe and efficient navigation, the navigation team uses a methodology to aid the decision making process, known as the phases of navigation (Hareide and

Ostnes, 2017b) or Dynamic Navigation (DYNAV) (T Dobbins et al., 2016, Forsman et al., 2011). The conduct of safe and efficient planning is shown in Figure 3, and is an iterative process.

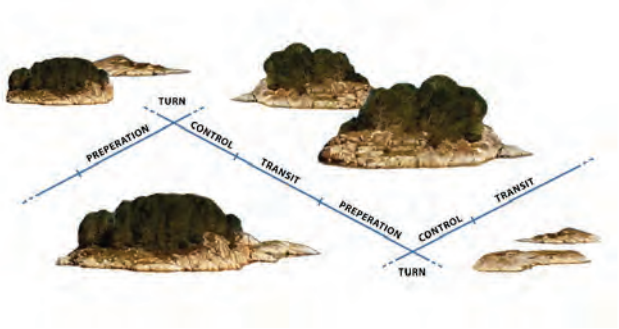


Figure 3: Iterative process of Phases of Navigation

In each phase of navigation, the navigator has a mental checklist to follow, and it is important that the navigators prioritize in order to have time to finish one phase before the next one starts.

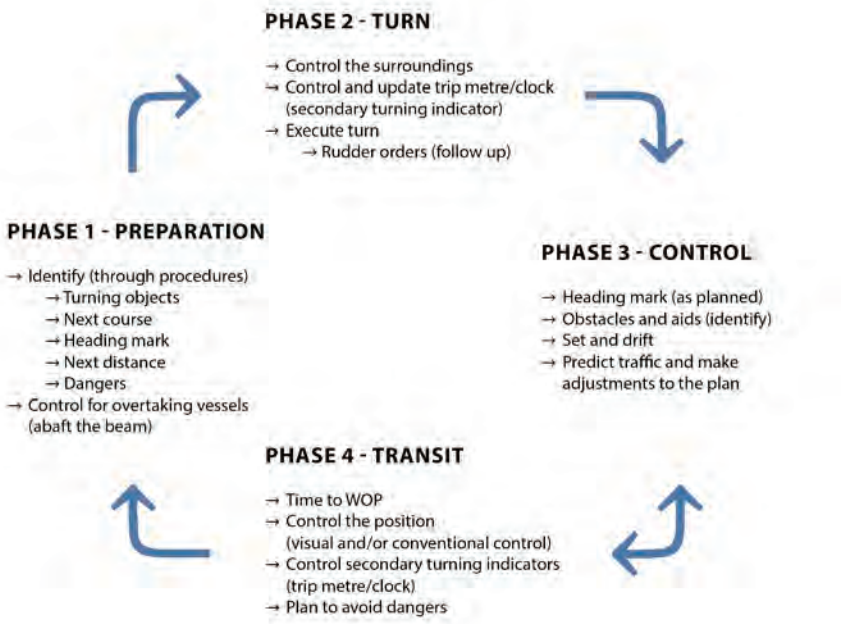


Figure 4: Phases of Navigation with example of checklist in each phase

The phases of navigation are a closed loop decision process, and if the navigator does not complete the process, measures must be taken to complete it. This could e.g. be reducing the speed.
Proper planning before conducting the passage facilitates an improved execution, and the standard operating procedures and the use of the phases of navigation is underpinned by the planning process.

2.1.1. NAVIGATION SYSTEM

Navigation systems on a modern vessel are networked, and the navigation sensors are integrated. The integrated information is presented on one or several MFDs, as shown in Figure 5.

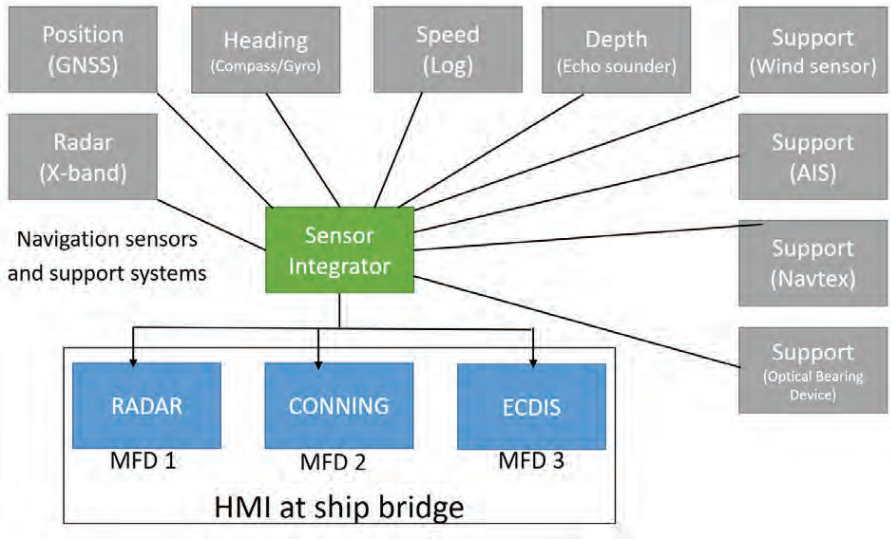


Figure 5: Navigation System

The integration of navigation sensors in the navigation systems aims to contribute to improved SA for the navigator, and thus support the safe navigation of the vessel. This is partly conducted by presenting the near real-time position of the vessel on the ECDIS. The information from the position-, heading-, speed-, depth- and support sensors are integrated and presented on one of the MFDs on the ship bridge. The three main applications available for the navigation team is ECDIS, radar and conning.

Signal interference on the signal from a Global Navigation Satellite System (GNSS), intentional or un-intentional, can lead to Hazardous Misleading Information (HMI) presented to the navigator (Last et al., 2010). There are several examples of jamming and spoofing of GNSS-signals (Glomsvoll and Bonenberg, 2017, Grant et al., 2009, Humphreys et al., 2008, Bhatti and Humphreys, 2014), and the navigator needs to be aware of the vulnerabilities in the computer system in use (Hareide et al., 2017a).

2.2. TODAYS GRAPHICAL USER INTERFACE

The phases of navigation are in place to ensure that the navigator is aware and appreciative of the current and future environment to support safe navigation. Figure 6 shows the idea behind the new route monitor window for presenting the navigator with need-to-know information of the current and future route (Hareide et al., 2017b).

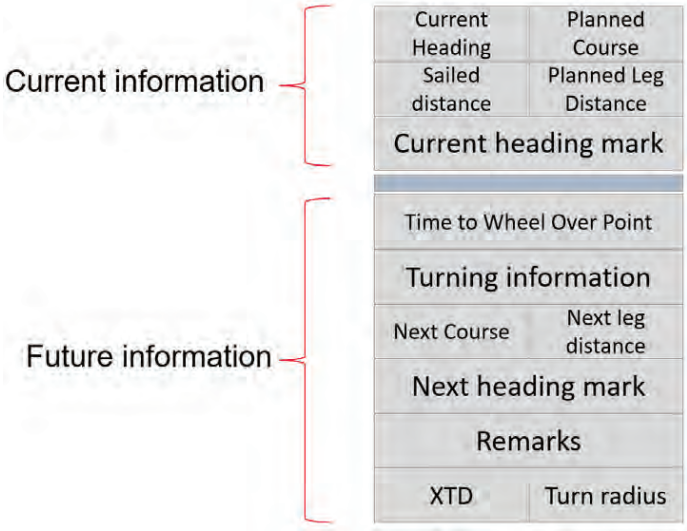


Figure 6: Conceptual content of route monitor window

Current information is presented on top (i.e. "what am I doing now"?) followed by future information (i.e. "what should I do next"?) on the bottom. Related information is grouped in sequences, limited by what kind of information that is necessary and sufficient to maintain maritime SA. This allows the navigators` scan pattern to flow from top-to-bottom and left-to-right with data presented in a readily usable form (DOD, 2012), avoiding critical data from being obscured by pagination or scrolling.

The coding used in turning- and heading mark information is in accordance with the Royal Norwegian Navy SOPs (RNoN, 2012), and a coding system has been made in order to facilitate for the presentation of information relevant for the passage accessed through the route monitor window. This is the same information as was collected from the paper chart, and the coding facilitates the use in electronic navigation.

Today's GUI is shown in Figure 7.

Figure 7: Today`s route monitor window

2.3. TOMMORROWS GRAPHICAL USER INTERFACE

Research has shown that the route monitoring GUI is not optimized, and that the use of MFDs induce HDT for the navigator (Hareide and Ostnes, 2018). Continuous control of the surroundings of the vessel is essential. This implies that the amount of HDT should be minimized in order to facilitate safe navigation. To some extent accidents at sea are caused by human error during navigation or critical operation. It is a paradox that continuously increased information flow challenges the crew's mental capacity by the fact that it is presented incoherently in many interfaces, thereby drawing the attention away from the real events outside the window.

Utilizing Augmented Reality, e.g. with the Microsoft Hololense, can provide information presentation augmented on the actual view out of the windows of the bridge for the navigator. This could drastically reduce HDT, and could thus improve safety. An example of a Maritime Augmented Reality (M-AR) GUI is shown in Figure 8:

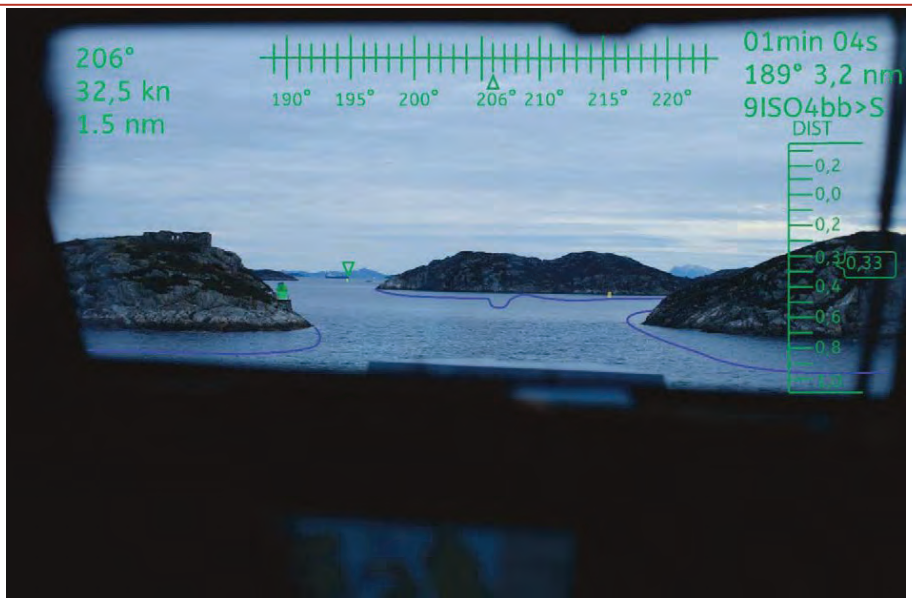


Figure 8: Example of M-AR GUI

The same information as presented in the route monitor window GUI in Figure 6 and 7 is present in the above Figure, but the navigator can collect all vital information related to the route monitor window while controlling the surroundings of the vessel. The use of this technology is the maritime domain is still immature, and there are several challenges with the use of it, but the use of AR will contribute to a reduction in HDT (Grabowski, 2015, Procee et al., 2017, Grabowski et al., 2018). The use of AR in this project so far, indicates more availability of data than the experience with the use of Head Up Displays (HUD) in the line of sight for the navigator.

3. CONCLUSION

The information management for the maritime navigator has not been given sufficient attention in order to make an efficient scan pattern, and there are indications of an increase in HDT for the navigator.

The standard operating procedure when conducting a passage is continuously to check the position with more than one mean, for example by using visual means. This is supported by the planning process, and the information must be presented in an unambiguous way to the navigator on the bridge. The importance of the information management will increase with more complex navigation scenarios, such as littoral waters, high speeds and during night hours.

The further aim for the information management should be to reduce the HDT, and this could be done by augmenting the visual scene of the navigator by using Augmented Reality. The technology has a high readiness level, but has not been tested sufficiently within the maritime domain to prove its usability. Further research and development will prove if AR will contribute to a higher level of SA for the navigator.

4. REFERENCES

Bhatti, J. & Humphreys, T. E. 2014. Covert control of surface vessels via counterfeit civil GPS signals. *University of Texas, unpublished*.

Da Conceição, V. P., Dahlman, J. & Navarro, A. What is maritime navigation? Unfolding the complexity of a Sociotechnical System. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 2017. SAGE Publications Sage CA: Los Angeles, CA, 267-271.

Dod, U. S. 2012. Design Criteria Standard, Human Engineering, MIL-STD-1472G. *In:* DEFENCE, D. O. (ed.).

Forsman, F., Dahlman, J. & Dobbins, T. Developing a Standard Methodology For Dynamic Navigation in the Littoral Environment. Royal Institute of Naval Architects, International Conference, Human Factors in Ship Design and operation, 2011.

Glomsvoll, O. & Bonenberg, L. K. 2017. GNSS jamming resilience for close to shore navigation in the Northern Sea. *The Journal of Navigation,* 70**,** 33-48.

Grabowski, M. 2015. Research on wearable, immersive augmented reality (wiar) adoption in maritime navigation. *The Journal of Navigation,* 68**,** 453-464.

Grabowski, M., Rowen, A. & Rancy, J.-P. 2018. Evaluation of wearable immersive augmented reality technology in safety-critical systems. *Safety Science,* 103**,** 23-32.

Grant, A., Williams, P., Ward, N. & Basker, S. 2009. GPS jamming and the impact on maritime navigation. *The Journal of Navigation,* 62**,** 173-187.

Hareide, O. S., Jøsok, Ø., Lund, M. S., Ostnes, R. & Heikala, K. 2017a. Enhancing Navigator Competence by Demonstrating Maritime Cyber Security. *Journal of Navigation,* In Review.

Hareide, O. S., Mjelde, F. V., Glomsvoll, O. & Ostnes, R. Developing a High Speed Craft Route Monitor window HCI International 2017, 2017b Vancouver. Springer.

Hareide, O. S. & Ostnes, R. 2017a. Maritime usability study by analysing Eye Tracking data. *The Journal of Navigation***,** 1-17.

Hareide, O. S. & Ostnes, R. 2017b. Scan Pattern for the Maritime Navigator. *TransNav 2017***,** 10.

Hareide, O. S. & Ostnes, R. Validation of a Maritime Usability Study with Eye Tracking Data. HCI International, 2018 Las Vegas. Springer, 23.

Hareide, O. S., Ostnes, R. & Mjelde, F. V. 2016. Understanding the Eye of the Navigator. *European Navigation Conference.* Helsinki.

Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'hanlon, B. W. & Kintner Jr, P. M. Assessing the spoofing threat: Development of a portable GPS civilian spoofer. Proceedings of the ION GNSS international technical meeting of the satellite division, 2008. 56.

Last, D., Grant, A. & Ward, N. Demonstrating the effects of GPS jamming on marine navigation. 3rd GNSS Vulnerabilities and Solutions Conference, Croatia, 2010. 5-8.

Norris, A. 2010. *Integrated Bridge Systems vol 2 ECDIS and Positioning,* London, Nautical Institute.

Procee, S., Borst, C., Van Paassen, M., Mulder, M. & Bertram, V. 2017. Toward Functional Augmented Reality in Marine Navigation: A Cognitive Work Analysis.

Rnon 2012. SNP 500. *In:* CENTRE, N. C. (ed.). Bergen: Royal Norwegian Naval Academy.

T Dobbins, J Hill, T Brand, Thompson, T. & Mccartan, S. 2016. Standardised information architecture to support the Dynamic Navigation (DYNAV) Standard Operating Procedure. *The Royal Institution of Naval Architects* 7.

Enhancing Navigator Competence by Demonstrating Maritime Cyber Security

Odd Sveinung Hareide, Øyvind Jøsok, Mass Soldal Lund, Runar Ostnes and Kirsi Helkala

Maritim sikkerhet har blant annet handlet om evnen til å gjennomfore sikker og effektiv navigasjon på havet. Sjøforsvaret har gjennom årene implementert gode rutiner for utdanning, opplæring, trening og øving av besetninger om bord pa Sjøforsvarets fartøyer for å kunne gjennomføre sikker og effektiv navigasjon.

De siste arene har det vart en økt interesse internasjonalt om begrepet Maritim Cyber Security (MCS). Det skrives mye bade i media og hos konsulentselskaper, uten at det finnes mye konkrete bevis eller demonstrasjoner som sier noe om hva dette begrepet innbefatter.

Spørsmålet vi har stilt oss er om den økte betydningen av datateknologi skaper nye sikkerhetsutfordringer som må tas hensyn til?

For å finne ut av dette har vi i 2017 gjennomført et prosjekt som har til hensikt a finne mer ut om sårbarheten til navigasjonssystemet til Sjøforsvaret, og om det er mulig a gjennomfore såkalte cyberangrep mot dette systemet.

MCS prosjektet er et samarbeid mellom Sjøforsvaret, Cyberforsvaret og KDA.

THE JOURNAL OF NAVIGATION, Page 1 of 15. © The Royal Institute of Navigation 2018
doi:10.1017/S0373463318000164

Enhancing Navigator Competence by Demonstrating Maritime Cyber Security

Odd Sveinung Hareide[1,2], Øyvind Jøsok[3,4], Mass Soldal Lund[3], Runar Ostnes[5] and Kirsi Helkala[3]

[1](*Norwegian Defence University College, Royal Norwegian Naval Academy, Navigation Competence Center, Bergen, Norway*)
[2](*Norwegian University of Science and Technology, Joint Research Program in Nautical Operations, Norway*)
[3](*Norwegian Defence University College, Cyber Academy, Lillehammer, Norway*)
[4](*Child and Youth Participation and Competence Development Research Program, Inland Norway University of Applied Sciences, Lillehammer, Norway*)
[5](*Norwegian University of Science and Technology, Department of Ocean Operations and Civil Engineering, Aalesund, Norway*)
(E-mail: oddsveinung.hareide@sksk.mil.no)

As technology continues to develop, information and communication technology and operational technology on board ships are increasingly being networked, and more frequently connected to the Internet. The introduction of cyber systems changes the work environment with the aim of decreasing the workload for the navigator, but at the same time introduces more complexity and vulnerabilities that in turn may alter the competencies needed to perform safe and e cient navigation. Contemporary examples of how cyber-attacks can distort situational awareness and interfere with operations are needed to enhance the navigator's competence through increased system awareness. This paper demonstrates some of the possible attack vectors that a cyber-attack can present to a ship, as well as discussing the plausibility and consequences of such attacks. In this study we provide a practical example to better understand how one can demystify cyber threats in order to enhance the navigators' competence.

KEYWORDS

1. Maritime. 2. Cyber Security. 3. Human Factor. 4. Navigation.

Submitted: 27 October 2017. Accepted: 4 March 2018.

1. INTRODUCTION. *"For the first time in maritime history the positive correlation between capital spent and power is undermined, cyber-attacks are low cost alternatives to physical attacks which have the ability to cripple maritime operations."* (Fitton et al., 2015, p. 14). This statement summarises the current dilemma for the maritime domain, as it is beginning to experience the vulnerable side of reliance on Information and

Communications Technology (ICT). The craftsmanship of maritime operations has always been the ability to safely and e ciently navigate the oceans, traditionally performed more or less in isolation from the rest of the world (Fitton et al., 2015). With increased digitisation and advances in electronically aided navigation where systems are increasingly being networked and integrated, such as Electronic Chart Display and Information System (ECDIS), radar, Automatic Identification System (AIS) and the Autopilot (AP), the maritime domain is increasingly dependent on cyber systems for safe and e cient navigation. However, digitisation and convergence of ICT and Operations Technology (OT) (BIMCO et al., 2017), creates potential attack vectors for an adversary with intent, persistence and resources to interfere with maritime operations.

The current drive towards even more integration of sensors together with increased use of automation to enable, for example, remote monitored or remote-controlled operations, will potentially bolster the significance of such successful attacks in the near future. Over-reliance in some parts of the integrated navigation system can result in dangerous situations (Norris, 2010; MAIB, 2014), and not being prepared for a cyber-incident against navigation systems might lead to significant consequences (Gard, 2016). Scholars and industry have jointly called for more cyber security testing of maritime cyber systems, in order to raise awareness and identify the need to conduct appropriate training and education for personnel operating such systems (Fitton et al., 2015; Dyryavyy, 2014). Simultaneously suggesting that to mitigate both the threat of, and potential negative e ects of successful cyber-attacks requires investment in both technology and people (Fitton et al., 2015). Despite recent headlines in the media regarding the e ects of cyber-attacks in the maritime domain (Baraniuk, 2017; Demchak et al., 2017), there seems to be a lack of relevant examples demonstrating attack vectors and e ects of cyber incidents on maritime navigation systems. We argue that more examples of cyber-attack possibilities are needed to aid the conceptual development and understanding of Maritime Cyber Security (MCS).

This article will first explore the contemporary understanding of the emerging concept of MCS. We argue that the current awareness and understanding of cyber security in the maritime domain is insu cient. By using the concept of Situational Awareness (SA) as a measure of safe and e cient navigation, Sections 2 and 3 discuss how cyber systems make SA more complex for the modern navigator. Section 4 introduces a demonstration of MCS carried out for learning purposes at the Royal Norwegian Naval Academy. The main body of the experiment is demonstrating how a cyber-attack can be performed against a modern maritime navigation system. This section also includes the design of the study and data collection, both utilising the cyber kill chain model (Hutchins et al., 2011). Section 5 presents the findings from the experiment. Sections 6 and 7 discuss impacts and conclude the article.

2. MARITIME CYBER SECURITY.

2.1. *The emerging concept of MCS.* MCS is a combination of the two terms 'maritime security' and 'cyber security'. The first term; maritime security, has been argued to have no definite meaning, and subsequently relates to di erent concepts depending on the individuals attempting to make sense of it, or practice it (Bueger, 2015). Only relatively recently has the North Atlantic Treaty Organisation (NATO) included maritime security as an objective in its Alliance Maritime Strategy (NATO, 2011). Bueger (2015) further argues that: "*Maritime security can first be understood in a matrix of its relation to other concepts*,

such as marine safety, sea power, blue economy and resilience." (Bueger, 2015, p. 1), where each of these concepts points to di erent dimensions of maritime security. However, these concepts described in the Maritime Security Matrix (Bueger, 2015) emphasise mostly the physical domain characteristics of maritime security. As the maritime domain is utilising advancements in ICT, new vulnerabilities are introduced as the cyber domain[1] is emerging in importance (MoD, 2013). Further, as assets in the maritime domain are becoming more integrated with increased sharing of information between ICT systems, maritime security relies also on a mature understanding of cyber security to operate and navigate safely and securely.

The second term; cyber security, has its origin in information security. Information security is mainly concerned with securing the integrity, confidentiality and availability of information (Whitman and Mattord, 2011), while cyber security is mainly concerned with the availability and integrity of the cyber systems (Von Solms and Van Niekerk, 2013). A consequence is that cyber security, in addition to protecting information transmitted or stored using ICT, also includes securing networks, Hardware (HW) and Software (SW) from unauthorised or malicious use. When ICT and OT are merging in the maritime domain, cyber security transcends into the operational domain of the navigator. Recent examples highlight that cyber-attacks have the potential to impact in the maritime domain by crossing the borders of cyber-physical interaction, resulting in loss of revenue (Maersk, 2017), or even have the power to provoke collisions by manipulating navigation information (Humphreys et al., 2008; Bhatti and Humphreys, 2014). While catastrophic events as a result of cyber-attacks such as explosions or fire are unlikely, errors introduced in a critical system such as the ECDIS are more likely. Such incidents have already been reported, with one of the latest examples known as the Black Sea incident (Goward, 2017).

To summarise, MCS can be understood as a part of maritime security concerned with the protection from cyber threats of all aspects of maritime cyber systems, particularly concerning integrity and availability. In addition, MCS is concerned with the reduction of the consequences of cyber-attacks on maritime operations. Thus, the means of MCS are not merely technological, but also consist of information and people.

2.2. *Understanding MCS.* According to Fitton et al. (2015), three elements of maritime cyber security should be taken into consideration to understand and mitigate cyber-attacks: Information, People and Technology.

These three elements are intertwined in forming the contemporary maritime cyber domain and are further outlined in Section 3. Technology is important in navigation and the conduct of all types of maritime operations, but also renders possible the exchange of information between agents in the maritime socio-technical system. In addition to the three elements of MCS, introduction of cyber systems in the maritime environment extends the reach of the maritime domain itself (Fitton et al., 2015). ICT creates connections between di erent locations in real time, with the result that the maritime domain is now, to a greater extent, converging with other domains like air, space and land. Hence, one important feature of the cyber domain is the ability to decouple location and presence (Floridi, 2017), creating the possibility of influencing both people and information in and through the cyber domain from distant locations. Therefore, when considering the concept of maritime

[1] Cyber domain means an electronic information (data) processing domain comprising of one or several information technology infrastructures (MoD, 2013).

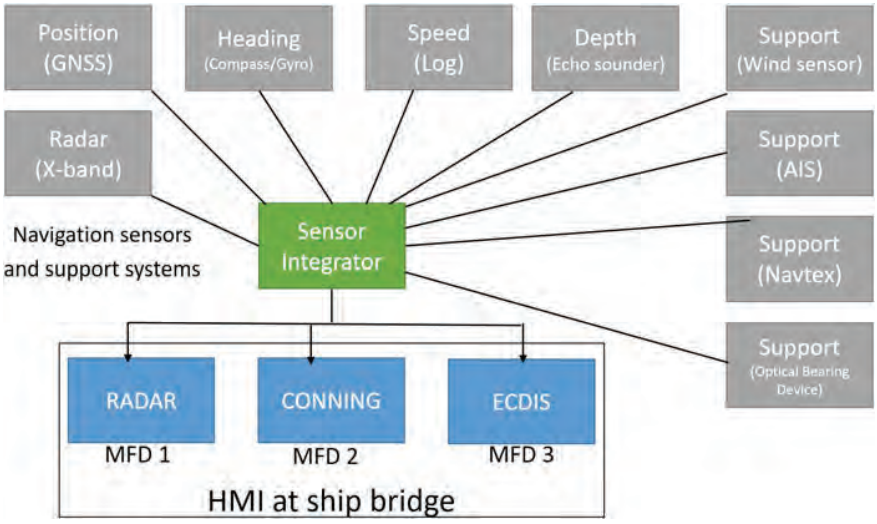


Figure 1. Example schematic of an integrated maritime navigation system.

security in the future, it will be vital to consider how the cyber domain is extending the maritime operating environment beyond a standard littoral boundary (Fitton et al., 2015).

By briefly exploring the features that cyber adds to the maritime domain, it is apparent that both the extended reach of the maritime domain and the mutual dependability between technology, people and information adds to the domain of interest for a navigator. This results in an extension of the SA requirements beyond the physically observable domain to conduct safe navigation.

3. SITUATIONAL AWARENESS FOR THE MODERN NAVIGATOR.

With the modern ship bridge, the maritime navigator has gone through a paradigm shift concerning the number and use of displays and sensors when conducting a passage. Historically, the main task for the navigator was to find and fix the position of the vessel, while today's navigator monitors the vessel's presented position on the ECDIS.

3.1. *Technology.*

The displays and sensors on board ships are connected using computer networks, known as Sensor Integrators (SINT). An example of how a maritime navigation system used by a navigator to conduct a passage could be integrated is shown in Figure 1.

The navigation system aims to provide information to increase the SA of the navigator in a timely manner. By providing an increased SA, the modern maritime navigation system enhances the safety of navigation by integrating information from sensors and provides augmented functions to avoid navigation accidents (Hareide and Ostnes, 2017a).

Navigation systems and sensors on board ships have been networked, and information increasingly integrated, for many years. The International Maritime Organization (IMO) has released a voluntary-fitted performance standard for Integrated Navigation Systems (INS), to set the minimum requirements for the equipment in use. IMO Resolution MSC.252(83) (IMO, 2007) describes the revised performance standards for INS, and the IMO recommends governments assure that an INS should be installed on ships built after

2011. There are several functions within the INS, and the aim is to utilise and combine these functions to provide "added value" for the operator to plan, monitor and control the safety of the ship during its passage (IMO, 2007).

The sensors and systems within an INS include, but are not limited by (IMO, 2007):

- The Electronic Position Fixing System (EPFS), providing the absolute position of the vessel (for example Global Positioning System (GPS)).
- Heading Control System (HCS), which enables the ship to keep a pre-set heading, known as an autopilot.
- Speed and Distance Measurement Equipment (SDME), providing the speed of the vessel (and thus distance).
- The ECDIS, used for chart presentation and presentation of relevant information for the navigator.
- Radar system, used as a mean for terrestrial positioning.
- AIS, automatic tracking system used on ships and by vessel tra c services (VTS).
- Echo Sounding System (ESS), providing the depth measurements for the vessel.
- Conning application providing information about the engine and manoeuvring status.
- Information distribution on Local Area Networks (LAN) and presentation of information on Multi-Function Displays (MFDs).
- Use of Communication channels such as Global Maritime Distress Safety System (GMDSS), which uses, for example, the NAVTEX receiver to receive navigational messages, or other communication channels for distributing data such as Satellite Communication (SATCOM) or mobile broadband.

The Maritime Cyber Security demonstrator presented in this paper shows an attack against an INS, but the attack would also be relevant against a networked and integrated maritime navigation system, even though not compliant with IMO Resolution MSC.252(83) (IMO, 2007).

3.2. *Information.* Concern has been raised about the modern navigators' ability to conduct proper monitoring of the systems in front of them. As an example, the term "playstation mode" (Hareide et al., 2016) has been introduced to visualise the concern about the navigator focussing more on the displays than the surroundings of the ship.

The e-Navigation concept was introduced to enhance safety of navigation and e - ciency of shipping (Hagen, 2017). e-Navigation is intended to promote safety, security and e ciency in global shipping, and a Strategic Implementation Plan (e-Nav SIP) has been introduced with a vision for e-Navigation (IMO, 2015). e-Navigation intends to meet users' needs through harmonisation of on board navigation and information systems, communication and supporting shore services. It is also expected that the level of automation will increase, and the number of displays will be reduced with implementation of e-Navigation. An example is the SMART e-Navigation project for integrating chart and navigation information for coastal ships in Korea (Kim and Park, 2016).

Today, the navigators' ability to determine and fix position is mainly conducted through EPFS, such as Global Navigation Satellite Systems (GNSS) and the most commonly used is GPS. GNSSs provide the absolute position of the vessel in more or less real time and have been a revolution for navigators. However, a navigator needs to be aware of several vulnerabilities such as signal interference and level of accuracy when using a GNSS. This

has led some to argue that the craftsmanship of navigation has decayed, because of an over-reliance on GNSS (Glomsvoll and Bonenberg, 2017; Norris, 2010). The craftsmanship of navigation for the modern navigator and the traditional navigator still shares at least one important factor of safe and secure navigation. The safe and secure navigation of a vessel relies on a navigator with a high level of Situational Awareness (SA). The purpose of e-Navigation and the INS is to provide the navigator with enhanced SA through timely and accurate information. However, with technological vulnerabilities introduced, we argue that the SA requirements also change.

3.3. *People.* A high degree of SA supports the handling of unexpected incidents (Wickens, 2002). According to Endsley (1995), SA has three constituent parts; perception, comprehension and prediction. The ability to develop and maintain a high level of SA varies significantly between people and tasks (Endsley and Garland, 2000) and when the cyber domain has entered the playground, Endsley's model of SA has been criticised for being too physical-domain oriented, missing vital features that the cyber domain brings (Alcaraz and Lopez, 2013). In the same vein, cyber-oriented SA papers have been criticised for being concerned with aspects related to SA that in fact are only sub-components, that is, sensors, recognised cyber picture, strategic picture, physical operations, etc., leaving the overall SA unmentioned (Franke and Brynielsson, 2014). According to Franke and Brynielsson (2014) the technical and cognitive sides of SA are closely related and somewhat intertwined, meaning that cyber information needs to be combined with other information to make sense and to obtain full understanding of the situation.

Wickens (2002) argues that in the context of aviation, the three components of SA are spatial awareness, task awareness and system awareness. The importance of awareness of the system has been mentioned by Adams et al. (1995) in relation to a growing concern of complex systems taking the operator partly "out of the loop". The maritime domain has similarities with aviation, and several of the conditions and restraints are coincident (Hareide and Ostnes, 2017a). Spatial awareness consists of the environment to which the navigator must adhere, and incorporates all the variables that the navigator must address to conduct a safe and e cient passage. The maritime environment is dynamic, and variables will alter during the passage. A navigator must take into account the vessel's current task (mission), which consists of navigation, seamanship, communication with other internal and external agents to conduct the task and system management (for example fuel management). System awareness for a navigator consists of the ability to understand and be aware of the state of the systems on the bridge. In aviation, the pilot usually needs not to be aware of the system status, unless an unexpected situation arises (Wickens, 2002, p. 131). With the introduction of e-Navigation and cyber systems on board, a high degree of system awareness is increasingly important in order to maintain SA. Both the vessel and the maritime environment are complex and dynamic, as are the systems within the vessel. One of these systems is the INS (Figure 1), which a navigator operates continuously. The complexity of the system, often coupled with poor design, makes system awareness di cult to maintain (Sarter and Woods, 1995; Hareide and Ostnes, 2017b). When understanding the system, and in this specific context the INS, it is important to relate it to the integrity, confidentiality and availability of relevant and time-crucial information flowing on the network of the INS. Thus, MCS is related to a navigator's SA through system awareness, illustrated in Figure 2.

According to Endsley's theory, level three SA gives a person the ability to project future states and events (Endsley, 1995). In a cyber-security context this will be the ability to;

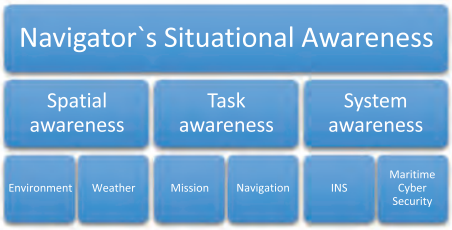


Figure 2. The relation between SA and system awareness. Note that the bottom line is meant as examples, and is not comprehensive as other examples could have been used.

"anticipate, detect and respond to unforeseen situations (failures or attacks) before they can cause disruptions" (Alcaraz and Lopez, 2013, p. 31). While this might seem too much to expect of a navigator, we think that simple e orts focussing on understanding and comprehension of the cyber threat could help mitigate large portions of contemporary cyber-attacks against an INS. With approximately 70% of breaches exploiting non-technical vulnerabilities (Deutscher et al., 2017), a navigator cannot a ord to disengage in gaining cyber competence and leaving it to be the sole responsibility of the ICT department. Hence, there is currently a need to make the intangible cyber threat tangible, in order to add to the competence of the navigator instead of creating more confusion and uncertainty. *"Preventing, identifying and defending against cyber-attacks requires educating, training and drilling sta , so they can e ciently respond to attacks, spot errors and continue to operate under cyber-attack conditions"* (Fitton et al., 2015).

4. USING THE CYBER KILL CHAIN TO DEMONSTRATE A CYBER-ATTACK AGAINST AN INS. This project was conducted as a cooperation between state-actors and industry. In order to facilitate and conduct the MCS demonstrator, the composition of the working group was important, and a need for di erent types of Subject Matter Expert (SMEs) was identified. The working group in this project consists of one engineer from an ECDIS developer, two cyber specialists, one navigation specialist and three students. Two of the participants have served as sailors with the Norwegian Royal Navy. The project started in February 2017, data gathering was conducted in August 2017 and findings were analysed and discussed in the Autumn of 2017 with the project ending in late 2017. It may be possible to reduce the timeframe of a similar project by applying the initial findings from this paper.

4.1. *Data Collection.* An important resource is a vessel on which to conduct the cyber-attack. The vessel presented in this paper is equipped with Commercial Of The Shelf (COTS) computers with the Windows 7 operating system, and a commercially available INS delivered by a contractor as the target system. Data was collected in a real-time environment on board a ship fitted with an INS as shown in Figure 1. Figure 1 outlines the complexity and shows how several sensors are interconnected through a Sensor Integrator (SINT). The navigation data is provided to the INS via a redundant LAN, providing all the MFDs with the information from the sensors interconnected through the SINT.

The passage was carried out during three days in late August, in Norwegian littoral waters in the vicinity of Bergen. The data collection was done around Bergen which had 87,156 port calls in 2015 according to Port of Bergen (POB) (POB, 2015).

The area is characterised by confined waters that are challenging for navigation, due to a high number of islands, skerries and underwater rocks. For the purpose of the experiment the procedure was documented by means of video recording and pictures. This documentation will not be presented in this article in order to anonymise the vessel and the manufacturers.

The first step was to gather the participants for an initial workshop where the overall concept for the study was discussed. In order to make swift progress the workgroup decided to separate the technical and operational part of the project, leaving one part working on how to spoof the ship's position presented in the INS from a technical point of view, and the other part working on the plausibility of gaining access and discussing operational consequences.

The exploration of the competencies needed to navigate in the twenty-first century, with regard to implications caused by the cyber threat, can be performed by thinking as if you are the potential attacker. This can be achieved by using the Cyber Kill Chain from Lockheed Martin (Hutchins et al., 2011) as the conceptual framework which consists of seven phases:

1. *Reconnaissance* such as harvesting email addresses, conference information, etc.
2. *Weaponisation* such as exploiting a backdoor in a system to achieve a deliverable payload.
3. *Delivering* a weaponised bundle to the victim via email, web, Universal Serial Bus (USB), etc.
4. *Exploiting* a vulnerability to execute code on a victim's system.
5. *Installing* malware on the asset.
6. *Command and Control* channel for remote manipulation of victim.
7. *Actions on objectives* conducted with "hand on keyboard" access, intruders accomplish their original goals.

4.2. *Reconnaissance.* The first part of the Cyber Kill Chain is reconnaissance. This was conducted in a workshop where the participants brainstormed potential attack vectors of the system. The participants in the workshop had in-depth knowledge of the technical and operational aspects of the system, navigational practice and routines regarding updates of HW and SW on board the specific vessel. In this initial phase we decided that spoofing the position provided by the EPFS by a small amount would be one plausible goal of an adversary with intent and capacity. The e ect could be bolstered by triggering the o set at a predefined point or by means of a remote command utilising the INS's merging of auxiliary systems such as AIS or NAVTEX (Figure 1). By drawing o knowledge about the updating routines and SME's system knowledge, an array of di erent cyber-attack vectors was identified. These vectors can be roughly be divided into two: firstly, if one has direct access to the system and secondly, if one can gain indirect access to the system. For the purpose of this project we decided to analyse what could be possible if we had direct access to the system and discuss the plausibility of gaining indirect access. The discussion was conducted by analysing the routines performed by developers, technicians and operators with access to the on board computers used in the INS (known as Operator Stations – OS). From an operational perspective, both an indirect access and direct access are plausible vectors of attack. The identified attack vectors are illustrated in Figure 3.

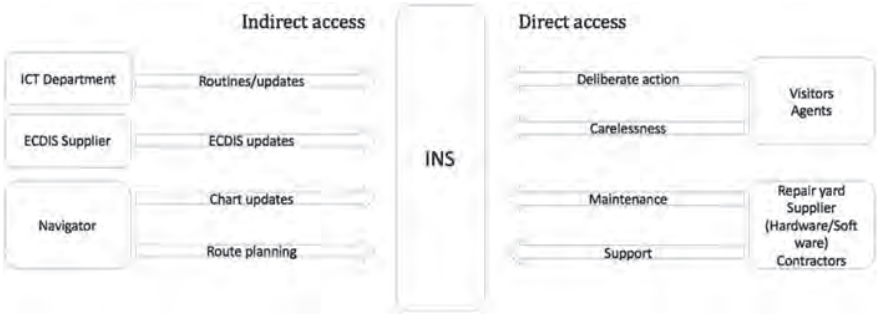


Figure 3. Potential attack vectors towards the INS.

The attack vectors are in general the same for all vessels, but there will be some differences when it comes to the age and maintenance routines of different types of vessels. Figure 3 provides an example of how one could map the different possible threat vectors within the MCS domain for a vessel. These attack vectors assume the INS does not have any outbound connections. However, reports (Dyryavyy, 2014; Baranuik, 2017) indicate that connecting the INS to the internet is becoming increasingly common, providing even more attack vectors.

4.3. *Weaponisation.* The weaponisation phase was performed by the cyber specialist by utilising open source information on how to develop the attack (Lund et al., 2018, in review). The cyber specialist used a laptop with the current windows version and the ECDIS application installed in order to test the attack during development. The rest of the participants engaged in conceptualising the notion of maritime cyber security and conducting focus groups with navigators to disclose cyber security awareness and current routines, and understanding of routines to mitigate cyber threats.

4.4. *Delivery, exploitation and installation.* Ways of gaining access to the system were identified in the initial workshop and the potential access points are shown in Figure 3. Once the attack was properly developed it was delivered through a USB port using a specially built USB device. First the USB device acted as a mouse and keyboard to log out of ECDIS and enter the operating system. The malware was installed on the Windows operating system and the computer was restarted. Once installed, the malware acted as "a man in the middle" between the sensory data input and the ECDIS application. The duration of this procedure was 5 minutes and 17 seconds, however improving the delivery could reduce the time needed to infect the system (Lund et al., 2018, in review). The end state is an ECDIS that seemingly has no faults and works as normal. Using the VirusTotal site (www.virustotal.com), the malware was tested against 60 of the most common anti-virus programs available for purchase. Only two of these detected any suspicious code in the malware, while the remaining 58 categorised the malware as "clean". An anti-virus program installed would therefore not be sufficient protection against a tailored cyber-attack like this.

4.5. *Command & control and action on objectives.* The INS is usually considered as an offline system. Therefore, command and control communication between malware and attacker through an Internet connection is not possible. In order to solve this problem, the malware was programmed to trigger at a specific position, so that when the ship crosses this predefined line, the malware starts to inject faulty values. In this case, the result is the ECDIS showing an increasingly faulty position.

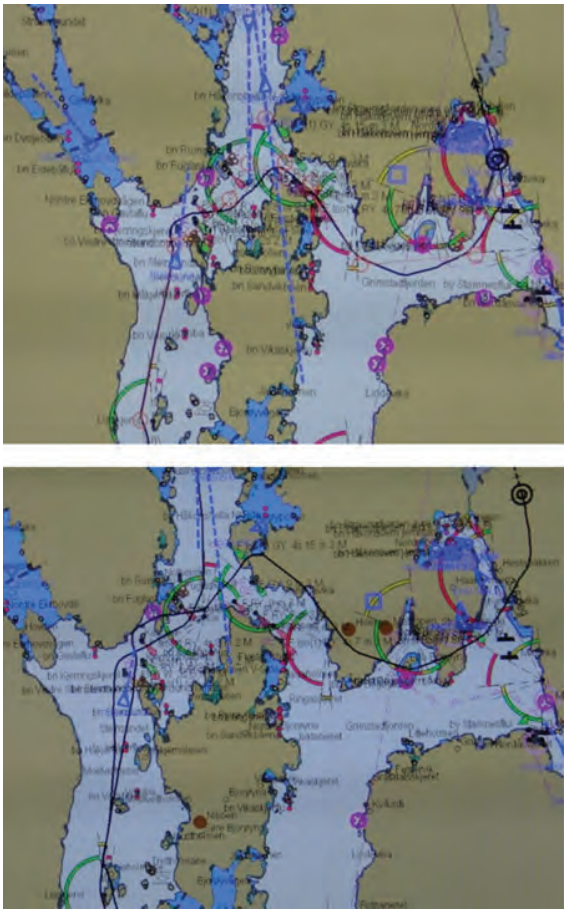


Figure 4. Upper print screen picture shows the ships actual track, lower screen picture shows the infected operator stations ship track.

5. FINDINGS. The malware was successfully installed on the computer by putting the USB device into an open and available USB slot. The full technical procedure is explained in Lund et al. (2018, in review). The malware was installed on the computer running the ECDIS SW, and successfully manipulated the GPS input causing the ECDIS to present a faulty position during the passage.

The malware was triggered when the ship crossed a predefined and pre-programmed position in latitude (lat) and longitude (long). The displayed position during this experiment was o set with at a rate of 0·0004 minutes (approximately 0·8 metres) per second towards the northeast (045°). This can be viewed in Figure 4, which shows the ECDIS, where the lower picture is spoofed, and the real position can be viewed in the upper picture.

A shutdown of the navigation computer was performed by triggering the malware at a second predefined position (lat/long), leaving the navigator unable to restore the proper ECDIS function during the passage. When restarting the computer, the malware hampered the SW's ability to operate, implied by a "blue screen".

The attack was also conducted when the vessel operated in “track mode”, which means that the autopilot is following the pre-planned route. When the position was spoofed, the autopilot corrected the spoofing by turning the vessel, thus taking the vessel away from the actual pre-planned route, which would eventually result in a “controlled” grounding of the vessel.

6. DISCUSSION. The introduction of ICT in the maritime domain expands the notion of maritime security by introducing cyber domain challenges. Therefore, it is fair to say that MCS has to be included as a part of maritime security measures. However, the cyber domain is crossing cyber-physical borders and hence cannot be treated as a technological issue alone. The implication of this insight is that maritime cyber security has to be considered as something more than an ICT department issue; it also includes people and information. As proven in our demonstration, the most crucial phase of a cyber-attack is the reconnaissance phase where an attacker utilises whatever means are available to gain critical information about the target system. This can include information available online, information gained through social engineering or even by gaining physical access to the target system. Hence, being o -line does not exclude the possibility of being exposed to targeted attacks. From a MCS perspective this means that if one can deny a threat actor information in the reconnaissance phase, this will reduce the risk of eventually experiencing an attack. However, this seems to be reliant on a combination of measures including enhancing competence of personnel operating the systems; in this case the navigator.

Introducing the cyber domain in the maritime context changes something; it adds something. It adds complexity and dependency on technology (for example, the removal of paper charts), and the operator’s competence requirement is changing from traditional navigation with analogue tools to also requiring digital competence and system awareness. This leads us to evaluate if introducing INS and e-Navigation also changes the competence requirements for the navigator. The demands for spatial and task awareness may be similar, while demands for system awareness change. This can be exemplified by comparing the “use of ECDIS” and the “understanding of ECDIS”. Today one could argue that the first is the focus, to use and harnessing of the advantages of the INS. However, from a competence perspective; to use and to understand the system is two di erent approaches to education and training. The need for a high degree of situational awareness is essential to be able to make good informed navigation decisions. When introducing INS and enabling the cyber domain we add the need to be situationally aware of the status of the system and the limitations and possibilities it presents. If one lacks system awareness, one would lack a vital part of the overall situational awareness and potentially present a risk factor rather than a risk reduction factor. So, in order to utilise the human capacity to be the strongest link in the MCS chain, MCS has to become a part of education and training in order to enhance the navigator’s competence by increasing system awareness. Using the cyber kill chain to conceptualise and demonstrate MSC can be a cost e cient and beneficial way to expose navigators to the threat and thus o er an easy solution to a growing challenge.

Our experiment demonstrates that cyber-attacks against an INS are relatively easily achievable. The security of the INS relies heavily on physical protection, while the INS itself is quite open once access has been established. Initially, the reconnaissance phase is the most resource-consuming for a potential attacker. This is where the attacker has to gain knowledge about the system and the routines of the crew in order to obtain information

such as passwords for login to higher maintenance levels, etc. However, ECDIS systems are available for purchase on the open market and technical documentation is relatively easily available, and sometimes even passwords can be available online (US-CERT, 2013). The discussion of whether this is possible is more a discussion about the attacker's intent, motivation, resources and persistence, than a discussion about whether this information is obtainable or not. Once the required technical documentation is obtained, an attacker would benefit from the ability to test the malware before installation. In this project our cyber specialist used less than two months' worth of man hours to achieve familiarisation with the system and to develop the attack. Even if the cyber specialist was given the ECDIS SW and had technical support from the supplier, this would also be within reach for a state actor or a large criminal organisation. The discussion then becomes if this would be plausible if the cyber specialist did not have the above-mentioned resources. It is quite clear that a teenager in his bedroom or a computer specialist in isolation would not have been able to perform such an attack.

Once the initial two phases are completed, the next critical phase is getting the malware installed. An ECDIS requires updates to sustain integrity over time, and in addition the ECDIS SW we used runs on a Microsoft Windows-based operating system that also requires regular updates and patching. The updating of charts and routes sometimes requires weekly or even daily updating and interaction between other computers through USB drives. Most vessels use ECDIS as an o ine system, and all updates are done by USB sticks. This results in a lot of interaction between the INS and auxiliary systems. Taking into account that the systems seldom have anti-virus and protective measures (Baraniuk, 2017), this leaves the operation of getting into the system with malware less demanding for an attacker. If direct access cannot be gained, an unknowing navigator or maintenance technician could potentially be used as the messenger, (see Figure 3). Once installed, the malware can trigger at a predefined position and therefore requires no more interaction with the attacker. The threat remains dormant until the activation criteria have been met.

The end state of this attack is to create uncertainty for the navigator when the position in the INS/ECDIS, and the observed position is not correlating. This may in turn reduce the navigators trust in the ECDIS and heighten workload if the position deviation is noticed (Hareide, 2013). This will reduce the quality of the navigator's SA, and it could contribute to a dangerous and undesirable event in relation to the navigation of the vessel. In a worst-case scenario the position deviation could be tailored to the ship and the waters in such a way that the deviation is di cult to detect and fast enough to run the ship aground.

For the navigator to better understand MCS, the conduct of the process as described in the cyber kill chain will establish a better system awareness, which in turn increases SA for the navigator and can contribute to the navigators' resilience in case of a cyber-attack. This will have implications for education and training of navigators, and we argue that an increased focus on system knowledge and understanding is needed with the changing working environment as more technology for the navigator is introduced. With an increased system awareness, the navigator will understand the importance of integrity monitoring and system awareness in the conduct of a passage.

7. CONCLUSION. This study explains and gives a working definition of Maritime Cyber Security and identifies the relationships between MCS and safe and e cient navigation through system awareness as a part of the navigator's overall SA. The importance

of high system awareness for a navigator operating the INS is laid down, as a contribution to increase the SA of the navigator. Further, the MCS demonstrator is explained and put into context.

Our demonstrator utilises the cyber kill chain to address the need to close the gap between the emerging threat of cyber-attacks and the competence needed at operator level. By utilising the cyber kill chain, the awareness of the emerging cyber threat to the maritime environment can be identified. When the threat is identified, measures can be taken to mitigate these threats. The demonstrator is a relevant example of how an actor with resources and motivation can spoof an INS.

By understanding the possibilities and limitations within the system in use, in this case an INS, an increased system awareness is developed and thus an increased SA and ultimately a safer and more e cient passage.

8. FURTHER WORK. The Original Equipment Manufacturer (OEM) of the equipment used in this study will patch the current SW by implementing our current findings in the existing SW, and the crew of the vessel will provide physical adjustments to on board equipment (for example lock-down procedures and use of anti-tampering tape) to prevent access to the system by outsiders (attackers). The findings from this study will be implemented in the current curriculum for maritime navigators at the Royal Norwegian Naval Academy to improve system knowledge and thus contribute to a higher level of SA. In future development of the demonstrated cyber-attack, we will investigate other vectors of delivery, as well as using the Automatic Identification System to exercise remote command and control of the malware.

ACKNOWLEDGMENTS

A special thanks to the Royal Norwegian Naval Academy and the Norwegian Defence University College, Cyber Academy, for support in conducting the work. We would also like to thank the crew of the vessel for facilitating the demonstrator and the OEM for contributing with system engineers.

FINANCIAL SUPPORT

The work was sponsored by the Norwegian Armed Forces CD&E grant EP1710 Concepts for CND in joint operation and the Royal Norwegian Naval Academy R&D grant.

ETHICAL STANDARDS

The authors assert that all procedures contributing to this work comply with the ethical standards of the relevant national and institutional committees on human experimentation and with the Helsinki Declaration of 1975, as revised in 2008. All details of the cyber-attack have been disclosed to the manufacturer of the INS.

REFERENCES

Adams, M.J., Tenney, Y.J. and Pew, R.W. (1995). Situation Awareness and the Cognitive Management of Complex Systems. *Human Factors*, **37**, 85–104.

Alcaraz, C. and Lopez, J. (2013). Wide-area situational awareness for critical infrastructure protection. *Computer*, **46**, 30–37.

Baraniuk, C. (2017). *How hackers are targeting the shipping industry*. Available: http://www.bbc.com/news/technology-40685821 [Accessed 22.08.2017].

Bhatti, J. and Humphreys, T.E. (2014). *Covert control of surface vessels via counterfeit civil GPS signals*. University of Texas, unpublished.

BIMCO, CLIA, ICS, Intercargo, Intertanko, OCIMF and IUMI. (2017). *Guidelines on Cyber Security onboard Ships*. *In:* BIMCO (ed.) Version 2.0 ed. Bagsvaerd.

Bueger, C. (2015). What is maritime security? *Marine Policy*, **53**, 159–164.

Demchak, C., Patton, K. and Tangredi, S.J. (2017). *Why Are Our Ships Crashing? Competence, Overload, and Cyber Considerations*. Available: http://cimsec.org/ships-crashing-competence-overload-cyber-considerations/33865 [Accessed 12.09.2017].

Deutscher, S., Bohmayr, W. and Asen, A. (2017). *Building a Cyber resilient Organization.* Available: https://www.bcgperspectives.com/content/articles/technology-digital-building-a-cyberresilient-organization/.

Dyryavyy, Y. (2014). Preparing for Cyber Battleships - Electronic Chart Display and Information System Security. NCC Group.

Endsley, M.R. (1995). Toward a theory of situation awareness in dynamic systems. *Human factors*, **37**, 32–64.

Endsley, M.R. and Garland, D.J. (2000). *Situation awareness analysis and measurement.* CRC Press.

Fitton, O., Prince, D., Germond, B. and Lacy, M. (2015). *The future of maritime cyber security*. Lancaster University.

Floridi, L. (2017). Digital's Cleaving Power and Its Consequences. *Philosophy & Technology*, Vol 30, 1–7.

Franke, U. and Brynielsson, J. (2014). Cyber situational awareness–a systematic review of the literature. *Computers & Security*, **46**, 18–31.

Gard. (2016). Cyber Security – managing the threat. Available: http://www.gard.no/Content/21112216/Cyber Security [Accessed September 2016].

Glomsvoll, O. and Bonenberg, L.K. (2017). GNSS jamming resilience for close to shore navigation in the Northern Sea. *The Journal of Navigation*, **70**, 33–48.

Goward, D. (2017). *Mass GPS Spoofing Attack in Black Sea?* Available: http://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea [Accessed 10.08.17].

Hagen, J.E. (2017). *Implementing e-Navigation*, Norwood, Artech House.

Hareide, O.S. (2013). *Control of ECDIS (electronic charts and display information system) on high speed crafts in littoral waters.* MSc, University of Nottingham.

Hareide, O.S. and Ostnes, R. (2017b). Maritime usability study by analysing Eye Tracking data. *Journal of Navigation*, **70**(5), 927–943.

Hareide, O.S. and Ostnes, R. (2017a). Scan Pattern for the Maritime Navigator. *TransNav 2017*, 10.

Hareide, O.S., Ostnes, R. and Mjelde, F.V. (2016). Understanding the Eye of the Navigator. *In:* NAVIGATION, N. I. O., ed. *European Navigation Conference, 2016 Helsinki. Confedent International*.

Humphreys, T.E., Ledvina, B.M., Psiaki, M.L., O'Hanlon, B.W. and Kintner Jr, P.M. (2008). Assessing the spoofing threat: Development of a portable GPS civilian spoofer. *Proceedings of the ION GNSS international technical meeting of the satellite division*, 56.

Hutchins, E.M., Cloppert, M.J. and Amin, R.M. (2011). Intelligence-driven computer network defence informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, **1**, 80.

IMO. (2007). Resolution MSC.252(83): Adoption of the Revised Performance Standard for Integrated Navigation Systems. London. Available: http://www.imo.org/en/KnowledgeCentre/IndexofIMOResolutions/Maritime-Safety-Committee-(MSC)/Documents/MSC.252(83).pdf

IMO. (2015). Draft e-Navigation Strategy Implementation Plan (SIP). *In:* 1/28, N. (ed.). Available: http://www.imo.org/en/ourwork/safety/navigation/documents/enavigation/sip.pdf

Kim, J. and Park, Y.-Y. (2016). An Integrated Approach to Korea's e-Navigation Communication Infrastructure. *International Information Institute (Tokyo). Information*, **19**, 643.

Lockheed Martin (LM). (2015). *Gaining the advantage*. Available: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/Gaining_the_Advantage_Cyber_Kill_Chain.pdf [Accessed 05.06.2017].

Lund, M.S., Hareide, O.S., Jøsok, Ø. & Skare, K.E. (2018). An attack on an integrated navigation system. USENIX Security Symposium, submitted, 2018.

Maersk. (2017). *Press release Interim Report Q2* 2017. Copenhagen. Available: http://investor.maersk.com/releasedetail.cfm?releaseid=1037421.

Marine Accident Investigation Branch (MAIB). (2014). *Report on the investigation of the grounding of Ovit in the Dover Strait*. Southampton. Available: https://assets.publishing.service.gov.uk/media/547c6f2640f0b60244000007/OvitReport.pdf

MoD, Finland. (2013). Finland's Cyber security Strategy. *In:* COMMITTEE, S. O. T. S. (ed.). Helsinki: MoD.

NATO. (2011). Alliance Maritime Strategy. Available: http://www.nato.int/cps/en/natohq/o cial_texts_75615.htm

Norris, A. 2010. *Integrated Bridge Systems vol 2 ECDIS and Positioning*, London, Nautical Institute.

Port of Bergen (POB). (2015). Annual Report. Available: https://bergenhavn.no/om-bergen-havn/arsrapporter/.

Sarter, N.B. and Woods, D.D. (1995). How in the World Did We Ever Get into That Mode? Mode Error and Awareness in Supervisory Control. *Human Factors*, **37**, 5–19.

US-Cert. (2013). Risks of Default Passwords on the Internet. *In:* SECURITY, D. O. H. (ed.). Available: https://www.us-cert.gov/ncas/alerts/TA13-175A.

Von Solms, R. and Van Niekerk, J. (2013). From information security to cyber security. C*omputers & Security*, **38**, 97–102.

Whitman, M.E. and Mattord, H.J. (2011). *Principles of information security*, Cengage Learning.

Wickens, C.D. (2002). Situation awareness and workload in aviation. *Current Directions in Psychological Science*, **11**, 128–133.

DEL 6

Fagfellevurderte artikler

Necesse 2018, Vol 3, Issue 2, 108-122 DOI: 10.21339/2464-353x.3.2.108

Lederskap, makt og cyber

Øyvind Jøsok[1,2]

[1] Forsvarets Høgskole, Forsvarets Ingeniørhøgskole, Lillehammer
[2] Høgskolen i Innlandet, Lillehammer
ojosok@cyfor.mil.no, ojosok@inn.no

Sammendrag. Militære operasjoner beskrives som stadig mer komplekse. I denne teksten drøftes cyberdomenet som drivkraft for denne utviklingen. Det argumenteres for at cyberdomenet har betydning for organisering av stridskreftene innen de tradisjonelle krigføringsdomenene i Norge; land, luft og sjø. Videre belyses det hvordan cyberdomenet griper inn i, og utfordrer, rådende forestillinger om maktstrukturer i Forsvaret, og i samfunnet ellers. Til slutt argumenteres det for at cyberdomenets økende betydning påvirker hvordan ledelse i Forsvaret utøves. Sentralt i argumentasjonsrekken står Forsvarets erfaringer fra satsning på nettverksbasert forsvar, Moses Náims bok; "The end of power" og General Stanley McChrystals bok; "Teams of teams". Kildene forenes i denne argumentasjoner gjennom fellestrekket hierarkisk tenkning i en nettverksbasert realitet.

Nøkkelord: Lederskap, Makt, Cyberdomenet, Cybermakt, Forsvaret

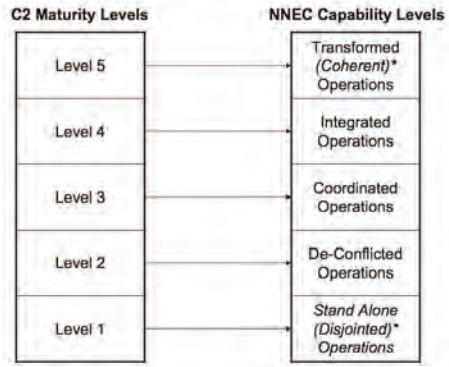
1 Hierarki og nettverk

1.1 Introduksjon

Det har lenge vært akseptert at det finnes like mange definisjoner av ledelse som det finnes mennesker som har prøvd å definere begrepet (Strand, 2007). Makt på sin side har i det egalitære Norge en noe negativ ladning (i motsetning til det engelske synonymet "power"), og dermed ofte tabu i samme setning som lederskap. Cyberdomenet på sin side er også et begrep som det hersker usikkerhet rundt betydningen av, og i hvilken grad det vil være et viktig element av fremtidige militære operasjoner (Lund, 2017). Muliggjør cyberdomenet militære operasjoner, eller er det et eget domene for militære operasjoner? Er cybermakt en realitet? Og har da cyberdomenet betydning for utøvelse av lederskap? I denne teksten vil de tre begrepene; lederskap, makt og cyberdomenet bli brukt i argumentasjonen, selv om det eksisterer svakheter i betydningen av det enkelte begrep. Argumentasjonen forsøker å rette fokus på hvordan disse begrepene påvirker hverandre, og hva de til sammen har å bety for utøvelse av ledelse i Forsvaret - nå og inn i fremtiden. Mer presist så vil følgende problemstilling bli drøftet: Hvordan påvirker cyberdomenet utøvelsen av lederskap i Forsvaret?

1.2 Nettverksbasering

Nettverksbasert Forsvar (NbF) har det siste tiåret vært et av de store satsningsområdene til det NATO. Allerede i 2002 ble de enighet i NATO C3 Board om å utvikle et NATO konsept som forente de ulike nettverksbaseringsinitiativene som fantes i alliansen (NC3A, 2005), og i 2010 ble NATO Network Enabled Capability (NEC) Command and Control Maturity Model utviklet (ACT, 2010). Denne modellen (Figur 1) beskriver fem nivå med tilhørende mål for graden av nettverksbasering, der nivå én er adskilte operasjoner, og nivå fem er fullintegrerte og nettverksbaserte operasjoner. Fundamentet for nettverksbasering er innføring av avansert nettverksteknologi.



Figur 1: NATO NEC Maturity Levels (ACT, 2010)

På Norsk side omtaler Forsvarets fellesoperative doktrine fra 2007 'evne til å operere i nettverk' og 'nettverksbasering' eksplisitt, og teknologiutviklingen innen informasjons- og ledelsessystem fremheves som en viktig driver for utviklingen (FFOD, 2007). Doktrinene fremhever nettverkstenking, sammen med effekttenking og manøvertenking, som det idémessige grunnlaget i militære operasjoner (FFOD, 2007). Videre defineres nettverkstenking som; "... å organisere sine ressurser mest mulig effektivt for å oppnå størst mulig systemintegrasjon, situasjonsbevissthet og forståelse av sjefens intensjon, og omfatter utvikling av mennesker, organisasjon og teknologi." (FFOD, 2007, s. 173). Etter modell fra NATO har først Sjef INI og deretter Sjef Cyberforsvaret vært ansvarlig for nettverksbaseringen av Forsvaret. FFOD (2007) setter også ambisjonsnivået for graden av nettverksbasert forsvar tydelig på agendaen:"Innledende NbF vil være innenfor rekkevidde i løpet av noen år. Et forsvar i denne fasen vil ha en organisasjon med gjennomgående gode kunnskaper om NbF, og NbF vil være en integrert del av all utdanning og trening." (FFOD, 2007, s. 97). I en evaluering av FFIs støtte til implementeringsprosessen konkluderes det med at det er vanskelig å si om fokuset på nettverksbasering av Forsvaret har gitt noen operativ effekt, eller om det bare har vært en naturlig forbedringsprosess (FFI, 2016). Det som forøvrig er interessant i konteksten 'cyberdomenets betydning for lederskap', er at rapporten fatter stor interesse for en vesentlig faktor; Nettverksbasering handler om å organisere i nettverk. Forsvaret er en sterkt hierarkisk organisasjon. Mennesker ser ut til å være flaskehalsen i denne spenningen, uten at det har vært gjort gode nok grep for å håndtere utfordringen under utdanning og trening av personell (FFI, 2016).

"Hvis militært personell er ment å tenke og handle i nettverk, så må de trenes og utdannes til dette. I dag tar all grunnleggende militær trening og tenkning utgangspunkt i hierarkier. Hierarkier er en grunnleggende annerledes måte å organisere arbeid på enn nettverk. For å bedre samhandling og kommunikasjonsflyt i Forsvaret, må menneskene i organisasjonen samhandle og kommunisere bedre og på andre måter enn det som er tilfellet i dag. Etter mange tiår med stor teknologioptimisme er det nødvendig å diskutere hvordan de mellommenneskelige utfordringene som er identifisert og definert kan endres, bedres og håndteres. I en militær kontekst er det nærliggende å peke på seleksjon, trening, utdanning og godt, gammeldags lederskap." (FFI, 2016, s. 33).

FFI (2016) peker her på et gap mellom visjonen nettverksbasert Forsvar og realiteten som preger organisasjonen.

1.3 Visjonen

Fra politisk nivå er det en tydelig uttalt ambisjon å satse på et høyteknologisk Forsvar (Se f.eks: (Prop. 151 Stortingsproposisjon, 2016); (Meld. St. Stortingsmelding, 2013)). Store materiellinvesteringer i alle grener (eks. F-35, Fregatt, oppgradering av CV90) vitner om evne og vilje til å investere i ny teknologi for å realisere visjonen. Utfordringen som bare vagt adresseres i FFOD fra 2007, og i liten grad i FFOD fra 2014, er at ved å investere i høyteknologiske plattformer og knytte disse sammen i nettverk, har man etablert en nytt domene på tvers av de eksisterende domenene; cyberdomenet. Cyberdomenet som operasjonsdomene er i seg selv interessant (Lund, 2017) men denne teksten vil ta for seg cyberdomenets påvirkning på andre deler av Forsvarets virke. FFI (2016)peker i sin rapport på mellommenneskelige utfordringer, Johnsen (2013) mener cyberdomenet utfordrer tradisjonelle forestillinger om organisering, FFOD (2014) påpeker at utviklingen utfordrer etablerte måter å lede på og Naím (2013) argumenterer for at den tradisjonelle forestillingen om makt endres. For å kunne besvare problemstillingen vil den videre teksten analysere de tre faktorene cyberdomenet, makt og lederskap med hensyn på spenningsfeltet mellom hierarki og nettverk.

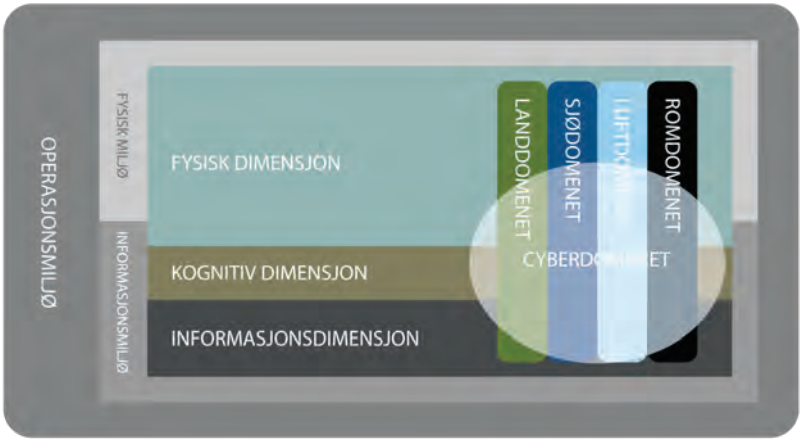
2 Cyberdomenet

2.1 En definisjon?

Bruken av prefikset cyber er ifølge Lund (2017) langt fra konsistent. Det fører til uklarheter når vi skal forholde oss til cyberdomenet som et domene for krigføring (Lund, 2017). Det finnes i dag en mengde definisjoner og begreper i den norske interessesfæren der enten cyberdomenet, eller lignende begreper for å beskrive det samme fenomenet, benyttes. NATO Cooperative Cyber Defence Centre of Excellence henviser til den Finske definisjonen av cyberdomenet (NATO, 2017). Den Finske versjonen er å finne i den Finske "Cyber Security Strategy" fra 2014 (MoD, 2013). Her defineres cyber-

domenet som: ”Cyber domain means an electronic information (data) processing domain comprising of one or several information technology infrastructures”. I FFOD (2014) omtales cyberdimensjonen, det datamaskingenererte rom og det digitale rom synonymt. Samme år omtaler Forsvarsdepartementet cyberdomenet i sine cyberretningslinjer (FD, 2014). Her defineres cyberdomenet som; ”Fysiske og logiske sammenkoblinger av informasjonssystemer, herunder nettverksenheter, kommunikasjonsinfrastruktur, lagringsmedier og data.” (FD, 2014, s. 4). Likheten mellom definisjonene som refereres til er at de belyser de teknologiske aspektene ved cyberdomenet. Spørsmålet som da gjenstår å besvare er om cyberdomenet bare er et menneskeskapt teknologisk domene, eller om det er noe mer. Lund (2017) trekker frem følgende betraktning: ”Cyberdomenet er en artefakt forma av intensjonane til skaparane, eigarane og brukarane av nettverk, system, maskinvare og programvare.” (Lund, 2017, s. 30). Dette er et perspektiv som belyser det faktum at en egenskap ved cyberdomenet er at det kan utnyttes på måter som domenet ikke er skapt for, eller intendert for (Lund, 2017). Noe som indikerer at cyberdomenet har egenskapen til å, direkte eller indirekte, påvirke andre domener og dimensjoner (Brangetto & Veenendaal, 2016).

Figur 2 er hentet fra NATOs pågående arbeid med å utarbeide en doktrine for cyberoperasjoner (AJP_3-20, Draft). Her spenner cyberdomenet over de fire tradisjonelle domenene - land, sjø, luft og verdensrommet. I tillegg spenner cyberdomenet over den fysiske dimensjonen, den kognitive dimensjon og informasjonsdimensjonen. Figuren viser at cyberdomenet kan påvirke både den fysiske sfæren til militære beslutningstagere, måten de forstår verden på, og den informasjon og kunnskap de er avhengig av for å kunne operere. I og gjennom cyberdomenet kan man altså i teorien påvirke og ramme både landoperasjoner, luftoperasjoner, sjøoperasjoner og operasjoner i verdensrommet på tvers av de tre dimensjonene. Et ganske altomfattende perspektiv. Samtidig illustrerer figuren at cyberdomenet i seg selv har fysiske, kognitive og informasjon attributter, i likhet med andre militære domener.



Figur 2: Gjengitt etter skisse i NATO AJP 3-20 (AJP_3-20, Draft)

Mangfoldet av definisjonen og begreper som brukes til å beskrive fenomenet som i denne teksten omtales som cyberdomenet er stort, noe som tyder på at den kognitive dimensjonen av cyberdomenet, altså forståelsen av domenet, er mangelfull. Selve cyberdomenet ser ut til å være i militær sammenheng noe prematurt og lite utviklet (Lund, 2017), iallfall i det Norske Forsvaret. Videre tyder det på at den fysiske dimensjonen av cyberdomenet fortsatt er underutviklet, siden Forsvaret ikke har nådd målene innen nettverksbasering med full sømløs integrasjon av alle plattformer, og dertil effektiv utveksling av informasjon for å understøtte beslutningstagere som skissert i FFOD (2014).

Figur 2 kan kanskje også illustrerer hvorfor cyberdomenet er et omdiskutert tema i militær sammenheng. I denne figuren fremstilles cyberdomenet foran og på tvers av de eksisterende krigføringsdomener. Denne fremstillingen utfordrer eksisterende tenkning og forståelse av militære operasjoner, og ikke minst etablerte hierarki og maktstrukturer innad i domenene. Selv om dette påpekes i FFOD (2014) som en konsekvens av nettverksbasering, er Forsvaret i økende grad tvunget til å ta innover seg at man må forholde seg til cyberdomenet på andre måter enn som muliggjører for samband mellom avdelinger og muliggjører for kommando og kontroll av militære enheter. Nettverksbasering har ført til etablering av cyberdomenet som i seg selv er et krigføringsdomene der makt kan utøves, eller projiseres gjennom (Haaster, 2016). Den part med best evne til å utnytte disse fordelene ved cyberdomenet vil kunne få store operasjonelle fordeler i militære operasjoner (Johnsen, 2013).

2.2 Cybermakt

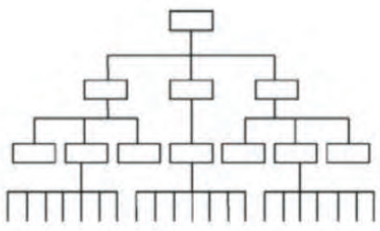
Innføring av luftmakt endret rollen til land og sjøstyrkene (Aron, 1955). Men selv om luftmakten var en realitet tidlig på 1900-tallet, var det i lang tid etterpå vanskelig å konseptualisere og konkretisere hva luftmakt egentlig var. Et sitat fra Winston Churchill i etterkant av andre verdenskrig illustrerer dette godt: “Air power is the most difficult of all forms of military force to measure or even to express in precise terms” Winston Churchill, 1948 (I Allen & Machain, 2017, s. 1). I 2017 ser det ut til at utviklingen av cybermakt følger en lignende bane. Erkjennelsen av cyberdomenet som krigføringsområde (NATO, 2016) og domenets potensiale som våpen (Johnsen, 2013), påvirker også rollen til de andre domenene. Selv om cyberdomenet har vært en realitet lenge, så er det fortsatt vanskelig å konseptualisere og konkretisere akkurat hva denne endringen er (Lund, 2017). Spørsmålet er fortsatt i hvilken grad, og hvilket omfang av endring, utviklingen av cybermakt vil utgjøre for de andre krigføringsområdene.

Cyberdomenet preges av både fysiske og ikke fysiske artefakter (Lund, 2017). Cyberdomenet knytter de ulike domenene sammen og muliggjør multi-domene operasjoner (Perkins, 2017). Samtidig visker cyberdomenet ut grensene mellom domener og dimensjoner i den forstand at det blir vanskeligere å skille mellom ”cause and effect”. Dette beskrives som mer kompleksitet i operasjonsmiljøet (McChrystal, Collins, Silverman, & Fussell, 2016). Dette fører til flere avhengigheter som må tas hensyn til, og det blir mer krevende å ha oversikt over alt som skjer innenfor domener og dimensjoner (Buchler et al., 2016). Disse egenskapene ved cyberdomenet gjør cyberdomenet egnet til, for en kapabel motstander, å påvirke andre domener i og gjennom den fysiske-

, kognitive- og informasjon dimensjonen som vist til i figur 2. Cybermakt er derfor ikke en triviell sak å definere på nåværende tidspunkt. De tilgjengelige definisjonene bærer preg av å inkludere alt. På den ene siden kan dette virke riktig med henvising til figur 2, men på den andre siden illustrerer dette også en slags avmakt i definisjonsprosessen der det fremstår usikkert hva cybermakt *egentlig* er, og hvilket omfang cybermakt har. I den videre drøftingen støtter denne teksten seg på følgende forståelse av cybermakt: *"Cyber power comprises the variety of powers affecting the geographic, physical network, logical, and cyber persona components, which consequently shape the experiences of state and non-state actors who act in and through cyberspace."* (Haaster, 2016, s. 14). Med henvisning til figur 2 kan cybermakt da forstås som å påvirke andre domener gjennom å utnytte den fysiske dimensjonen (f.eks ved å fysisk ta kontroll over nettverk), informasjonsdimensjonen (f.eks ved å bruke cyberangrep til å manipulere informasjon) eller den kognitive dimisjonen (f.eks ved å bruke sosiale media profiler til å påvirke) av cyberdomenet. Med denne forståelsen må cyberdomenet og cybermakt behandles som noe mer enn nettverksteknologi og cyberangrep.

2.3 Den menneskelige faktor

Innføring av nettverksbasert Forsvar, og dermed etablering av cyberdomenet, har handlet om teknologi (Andreassen, 2017). Det har handlet om å omstille et lavteknologisk invasjonsforsvar til et høyteknologisk innsatsforsvar. Men nettverksbaseringen har hatt begrenset effekt (FFI, 2016). I likhet med FFI påpeker Andreassen (2017) svakheter ved utdanning, trening og øving i forbindelse med nettverksbasering av Forsvaret. Det er indikasjoner på at det har vært og er klare skiller mellom innføring av teknologi, utdanning innen bruk av teknologi og det å lede i et nettverksbasert Forsvar, noe som fører til redusert og forsinket evne til å utnytte teknologi (Andreassen, 2017). Det har ikke vært tilstrekkelig investert i menneskene og konkret påpekes det svakheter innenfor samhandling og kommunikasjon (FFI, 2016). Noe som har ført til en forsinket evne til å ta i bruk ny teknologi. *"The delayed implementation of Network Based Defence affects the entire Norwegian Armed Forces and puts military lives and operations at stake"* (Andreassen, 2017, s. 19). Hva er det som gjør at samhandling og kommunikasjon reduserer effekten av NbF-satsningen? En grunn kan være at all grunnleggende militær utdanning i Forsvaret i dag tar utgangspunkt i hierarkier, og at dette er en grunnleggende annerledes måte å tenke på enn nettverk (FFI, 2016). En hypotese er altså at Forsvaret har prøvd å innføre nettverkstenking uten å endre måten vi tenker på.



Figur 3: Hierarki og nettverk (FFI, 2016)

Alle de tradisjonelle domenene i det Norske Forsvaret er organisert i hierarki. Cyberdomenet muliggjør fysisk og logisk sammenkobling i nettverk (Figur 3). Slik skapes nettverk, og nettverk av nettverk, innad i og mellom tradisjonelle strukturer. I tillegg til de formelle nettverkene, Forsvarets egne systemer, eksisterer også uformelle nettverk (F.eks bruk av mobiltelefon, sosiale media etc.) som skapes og utnyttes av Forsvarets personell for å løse oppdrag. Disse uformelle nettverkene har fått stadig større betydning og aksept som en normal del av militære operasjoner (trening, øving og skarpe oppdrag). Samtidig blir Forsvaret stadig mer avhengig av sivil nettverksinfrastruktur og sivile leverandører og underleverandører som utelukkende utnytter sivil nettverksinfrastruktur. Dette er et resultat av egenskapene til cyberdomenet. Cyberdomenet muliggjør sammenkobling og informasjonsutveksling, noe som er nyttig for kommando og kontroll, men det skaper samtidig utfordringer i den menneskelige dimensjonen både hva gjelder makt og lederskap. Noe som er tema i de to neste delene av teksten.

3 Makt

3.1 Makt i endring

"Power is the ability to direct or prevent the current or future actions of other groups or individuals. Or, put differently, power is what we exercise over others that leads them to behave in ways they would not otherwise have behaved" (Naím, 2013)

Moisés Naím (2013) argumenterer i sin bok "The end of power" for at makt gjennomgår en transformasjon der sentraliserte hierarkiske mastodonter taper makt til fordel for mindre uorganisert grupper eller individer. Han baserer sin argumentasjon på tre faktorer; 'more', 'mobility' og 'mentality'. Den første faktoren, more, innebærer det faktum at det i dag finnes mer av alt. Når det finnes flere mennesker, og disse har muligheten til å leve et mer tilfredsstillende liv, er konsekvensen at de blir vanskeligere å kontrollere. Individer kan i større grad være mobile fordi det er billigere, raskere og enklere å gjøre. Resultatet er at individ mikses sammen på tvers av kultur, religion og andre demografiske skillelinjer. De to forestående faktorene har resultert i at mennesker raskere endrer mentalitet. Mer kunnskap og kompetanse betyr at den enkelte krever mer og forventer mer av maktstrukturene som regjerer, på alle nivå (Naím, 2013). Naím attribuerer ikke denne endringen i makt til cyberdomenet alene, men argumentert for at cyberdomenet i økende grad er en arena for påvirkning og utøvelse av makt. Derfor er det interessant å se nærmere på hvordan makt og cyberdomenet påvirker hverandre i en militær kontekst.

Grunnleggende i utøvelsen av makt er at maktstrukturen må ha kapasitet til å kunne utøve denne makten. Det vil si evne og vilje. I militære strukturer har dette vært synonymt med kommando og kontroll. En formell tilgang på makt gjennom kapasitet (soldater og våpen) og formalitet (posisjon), og evne til å kontrollere utøvelsen av denne

(Forsvaret, 2012). Tradisjonelt har mer makt vært bedre enn mindre makt, og måleenheten har vært mengde og teknologi. Denne forståelse av makt er ifølge Naím (2013) i ferd med å endre seg radikalt. Han argumenterer for at endringene som følge av more, mobility og mentality favoriserer 'micropowers' og er i 'megaplayers' disfavør. Megaplayers er i denne sammenheng å betrakte som en nasjons eller koallisjons militærmakt, og micropowers små grupper eller individer som har evne og vilje til å nekte megaplayers å seire i en konflikt (Naím, 2013). Eksemplene på nettopp dette begynner det å bli mange av. Men likevel er den rådende oppfatningen at en teknologisk avansert militærmakt er essensielt for en nasjons sikkerhet (Naím, 2013), spørsmålet er om denne karakteristikken av makt er dekkende i den moderne konteksten: "Today, national armies are attempting to adjust - with different speeds and results - to "full spectrum" warfare in which weapons are digital as much as physical methods are psychological as much as coercive, and combatants are civilian and scattered as much as uniformed and coordinated" (Naím, 2013, s. 123).

3.2 Lende og tid

En av karakteristikkene som har endret seg er at konflikter i mindre grad er knyttet til fysisk territorium (Naím, 2013). Noe som også i høyeste grad er gjeldende for cyberdomenet og utøvelsen av cybermakt."Cyberpower gives the little guys the kind of ability that used to be confined to superpowers" (Amos Yadlin, 2009 i Naím, 2013). Dette er forøvrig ingen ny tanke, siden enhver militærteoretiker vil påstå at konflikter vinnes og tapes i det kognitive domenet[1] (FFOD, 2007). Cybermakt vil derfor kunne dele egenskaper med andre domeners forståelse av makt, forskjellen er derimot at 'lendet' er av en annen karakteristikk (Bibighaus, 2015). Her kan det argumenteres for at selve lendet er formbart i en større grad enn i de andre domenene, siden lendet (cyberdomenet) i seg selv er menneskeskapt (Lund, 2017). Det vil implisitt si at dersom man ikke har etablert cyberdomenet innad i f.eks en nasjon, vil det være umulig for en motstander å utøve cybermakt i og gjennom cyberdomenet for å påvirke opinionen. Noe som kan argumenters for er situasjonen i Nord-Korea, digitalisering av landet på et så lavt nivå at cyberdomenet ikke eksisterer (Naughton, 2017).

En annen karakteristikk som har endret seg, er tid, i dobbel forstand. Cyberdomenet er gjennom teknologisk utvikling alltid gjenstand for endring, rask endring. Som General Amos Yadlin påpeker; "Staying ahead of the game is important in light of the dizzying change of pace in the cyber-world, at most, a few months in response to a change, compared to the years pilots had" (Amos Yadlin, 2009 i Naím, 2013) Samtidig blir langsiktige initiativ med mål om å plante bakdører eller tilganger til systemer og nettverk for fremtidig bruk vanligere (F.eks Operation Nitro Zeus[2]). Konsekvensen blir

[1] Forsvarets Fellesoperative Doktrine (FFOD) bruker begrepet det kognitive domenet. Tidligere har det vært referert til den kognitive dimensjonen. Disse begrepene behandles som synonymer i denne teksten og har samme betydning.

[2] Operation Nitro Zeus er ikke bekreftet av offisielle kilder, men skal være i følge dokumentaren Zero Days (Gibney, 2016) være et initiativ fra amerikanske National Security Agency (NSA) med mål om å infiltrere Iranske våpen og datasystem i tilfelle eskalering av konflikten i kjølevannet av STUXNET angrepet.

at en motstander som har god tid, og evner å iverksette langsiktige initiativ, gjerne i årevis eller mer, er bedre til å utnytte cyberdomenet enn en som handler på impuls (Hutchins, Cloppert, & Amin, 2011). Konsekvensen er at i cyberdomenet er ikke overraskelse nødvendigvis knyttet til militære enheters manøver i øyeblikket, men kanskje til en manøver utført for lenge siden. En realitet som dette gjør at man i et 'worst case scenario' står i fare for å være utmanøvrert før striden har begynt.

3.3 Makt og struktur

Både FFI (2016) og Andreassen (2017) peker på at nettverksbaseringen til nå har gitt lite operativ effekt og at innføringen har gått sakte. Noe av svaret kan kanskje finnes i skillet mellom hierarki og nettverk, og makt. Hierarki betyr sentralisert kommando og kontroll, og sentralisert kommando og kontroll betyr makt. Nettverksbasering og nettverkstenking baserer seg på distribusjon av makt og desentralisert ledelse (FFOD, 2007). I dette grenselandskapet ligger kanskje noe av motsetningen mellom cyberdomenet og ledelse i Forsvaret å finne. To mulige forklaringer belyses:

1. Det å gå fra et veletablert hierarki med godt definert ansvar, roller, myndighet og oppgaver, til et mer løst organisert nettverk, betyr endring. Det kan oppleves som reduksjon i makt (Busch, Vanebo, & Dehlin, 2010). Organisering i mindre enheter på tvers av stridskrefter på tvers av hierarkiet, og til og med til andre sektorer, vil si et redusert handlingsrom dersom man ser på det hele med et konservativt hierarkisk mindset. En mulig løsning på dette problemet kan være å omdefinere den grunnleggende forståelsen av makt, som Naím (2013)foreslår. Dette vil sannsynligvis ikke skje så lenge man fortsetter å utdanne som i dag der "all grunnleggende militær trening og tenkning utgangspunkt i hierarkier." (FFI, 2016, s. 33). Til dels fordi kultur skapes, opprettholdes og endres på Forsvarets utdanningsinstitusjoner (FFI, 2016).
2. En mulig andre forklaring kan være at å gå fra et etablert hierarki til mer dynamisk nettverkstenking kan virke skremmende. Lavere grad av kontroll og høyere grad av usikkerhet knyttet til operasjonelle faktorer vil være realiteten, fordi multi-domene operasjoner vil være mulig (Jøsok et al., 2016). Dette har implikasjoner på hvordan militære lederutdanningen gjennomføres i praksis, og hva som ses på som nødvendig lederkompetanse i et mer dynamisk og komplekst miljø. Kanskje vil det handle mindre om prosedyrer og metoder, og mer enn å håndtere kompleksitet og raske kontekstskifter.

Cyberdomenet som muliggjører for nettverksbasering kan altså oppfattes som en trussel mot personlig makt, og være med på å skape frykt på grunn i overgangen fra hierarkisk tenkning til nettverkstenking. Den økte betydningen av cyberdomenet vil derfor ha konsekvenser for alle domener slik som figur 2 illustrerer, både organisatorisk og individuelt. Når vi tar inn over oss konsekvensen av more, mobility og mentality, er det i denne teksten mest interessant å se på hva dette har å bety for lederskap.

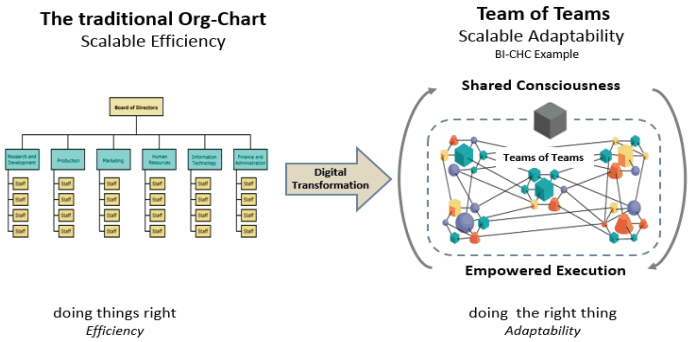
4 Lederskap

4.1 Ledelse av multi-domene operasjoner

Kapittel 2 og 3 har belyst at cyberdomenet skaper utfordringer internt i Forsvarets organisasjon i forhold til at vi må organisere oss annerledes og tenke annerledes, hvis vi skal fungere sammen i og gjennom cyberdomenet. Dette vil kreve nye former for kompetanse (Mld. Stor. Stortingsmelding, 2013). Eksternt skaper cyberdomenet problemer med å distribuere makt til mindre grupper som har evne og vilje til å bruke dette med ondsinnede hensikter. General Stanley McChrystal identifiserte hva dette hadde å si for lederskap gjennom sine erfaringer i Afghanistan: "it became clear to me and to many others that to defeat a networked enemy we had to become a network ourselves." (McChrystal, 2011). I likhet med FFI (2016), påpeker han at den hierarkiske tilnærmingen var uegnet til å håndtere utfordringene han møtte. Megaplayeren NATO kunne ikke hamle opp med micropoweren Al-Qaida. Et grunnleggende problem som McChrystal identifiserte, var motstanderens evne til å organisere seg adaptivt i celler, ofte på tvers av geografi og sammensmeltet med sivilbefolkning. I tillegg hadde motstanderen evne til å utnytte ny teknologi til å dele informasjon raskt og effektivt. Motstanderen viste også stor evne til resiliens, altså å komme seg på beina igjen etter å ha vært slått i et lag. Slik har innsatsen i Afghanistan blitt en dyr affære, som har gitt lite resultat sett opp mot de strategiske målsetningene som var satt for invasjonen. Motstanderen flyttet dermed krigen fra manøverkrigføring som styrkene var forberedt på med store hierarkiske organisasjoner, til counter-insurgency der mindre enheter og andre metoder var mer effektive enn den tradisjonelle krigsmaskinen. For det norske Forsvaret har det vært mange verdifulle erfaringer å hente fra Afghanistan. Men dessverre lite innen ledelse på operasjonelt nivå som Høiback påpeker: "I Norge faller kompetanseforvaltning og kompetanseutvikling utover det stridstekniske nivået utenfor det som vi oppfatter som militært relevant" (Høiback, 2017, s. 33). Norge har definert seg selv som en god alliert (NOU, 2016), men det er neppe nok til å utløse en gjennomgripende debatt som evner å endre lederpraksisen i Forsvaret slik at den kan tilpasses nettverkstenking og fremtidens utfordringer.

4.2 Stormester eller gartner

General McChrystal (2016) beskriver hvordan store organisasjoner må revitalisere seg selv på grunn av den digitale transformasjonen. Uavhengig om det er i næringslivet eller i krig, så identifiserer han at å respondere raskt og det å være tilpasningsdyktig, er kritiske kompetanser i en organisasjon. For å kunne håndtere utfordringene trengs nye kommunikasjonsformer og samarbeidsformer. "That requires new ways to communicate and work together" (McChrystal et al., 2016, s. vii). Konklusjonen til McChrystal er altså nærmest identisk med den FFI (2016) presenterer. McChrystals (2016) visualisering av konklusjoen er også nesten identisk med den FFI (2016) bruker i sin rapport. Cyberdomenet muliggjør nettverksbasering, og tvinger frem en endring fra hierarki til nettverk. Så hva vil dette har å si for lederskap?



Figur 3: Teams of teams (McChrystal et al., 2016)

Nok en gang påpeker McChrystal det som FFI påpeker; man kan ikke utdanne ledere til å fungere i et hierarki når man skal lede i et nettverk, og at dette krever en endring i hvordan ledelse og makt oppfattes. "...the mental transition from heroic leader to humble gardener was not a comfortable one. From the first day at West Point I'd be trained to develop personal expectations and behaviours that reflected professional competence, decisiveness, and self-confidence…. I felt intense pressure to fulfil the role of chess master for which I had spent a lifetime preparing. But the choice had been made for me. I had to adapt to the new reality and reshape myself as conditions were forcing us to reshape our force. And so I stopped playing chess, and I became a gardener" (McChrystal et al., 2016, s. 225).

Konsekvensen av more, mobility og mentality muliggjort av cyberdomenet, gjør verden mer kompleks. Det fører også til at militære operasjoner blir mer komplekse. Det er rett og slett flere faktorer som må tas hensyn til, og disse faktorene er sammenkoblet på nye og komplekse måter. Her er det et viktig skille mellom komplisert og komplekst. Kompliserte problem betyr at det er et relativt oversiktlig sett med variabler som må håndteres i en kontekst. F.eks manøverkrigføring mot en relativt kjent fiende. Komplisert problem som kan løses med å bruke tilgjengelige ressurser effektivt. Komplekst problem krever mer tilpasning, fordi prosedyrene du kan ikke passer til problemet. Derfor kommer McChrystal til konklusjonen at "Adaptability, not efficiency, must become our central competence." (McChrystal et al., 2016, s. 20). Og dette handler om lederskap på flere nivåer. FFI påpeker at det handler om "godt gammeldags lederskap" (FFI, 2016, s. 33). Det betyr ikke at man skal lete frem "Veiledning i militært lederskap fra 1974" og begynne å lese den. Det handler om at alle nivå av ledelse i Forsvaret må innse at lederskap endrer seg i takt med innføring av teknologi og nettverksbasering. Det er ikke effektivt å opprettholde eksisterende maktstrukturer og basere seg på kommando og kontroll i møte med nye utfordringer drevet av f.eks. cyberdomenet. Lederkompetanse er ikke lengre å ha full kontroll på alle stegene og håndverket i alle ledd i organisasjonen. Endringene i Forsvarets organisasjon er allerede for raske til at dette er tilfellet. Lederkompetanse er derfor også i endring. Utfra argumentasjonen i denne teksten er det nødvendig med en dreining mot om å bygge integritet på å gi fra seg makt,

fremfor å sentralisere makt, og dyrke de rundt seg slik at samhandling og kommunikasjon kan finne sted. I en multi-domene kontekst, der domener og dimensjoner smelter sammen, kan vi ikke tillate oss å redusere militært lederskap til en forestilling om at målet er å bli stormester i sjakk.

4.3 Konsekvenser for lederutdanning

Det å gjøre organisatoriske endringer for å tilpasse konsekvenser av cyberdomenets økte betydning, handler i tillegg til organisatoriske og strukturelle endringer, om å ta bevisste valg rundt hvilken kompetanse man tilfører personellet i organisasjonen gjennom utdanning, trening og øving. Det finnes i dag lite beviser på at lederutdanning og lederutvikling fungerer i Forsvaret. Det finnes derimot indikasjoner på det motsatte; at det ikke fungerer, at det er tatt lite bevisste valg og at lederutviklingsstrukturer er redusert (Luktvasslimo, 2013). Et annet eksempel er at kadetter kan beskrives som mindre modne når de uteksamineres enn når de begynner på skole i Forsvaret (Strengen, 2014). Dette kan være en indikasjon på at man prøver å lære bort lederskap som et sett egenskaper, holdninger, ferdigheter og metoder som tilpasses den gjeldende konteksten. Gjerne ved forelesning og deretter praksis hvor man får tilbakemelding på om det er riktig eller feil. Sett i lys av argumentasjonen i denne teksten, fremstår dette som en utdatert forståelse av lederskap, utøvelse av ledelse og det å lære å lede. Feilene her er mange. Forestillingen om manøverkrigføring ligger til grunn for alle militære operasjoner, og man i stor grad forholder seg til stridsteknisk nivå i utdanning av nye ledere. Endringene i cyberdomenet bringer med seg, betyr at nivået må heves (i dobbel forstand) på lederskapsutdanningen tidligere. Først opp fra stridsteknisk til operasjonelt og strategisk, slik at flere ledere forstår koblingen mellom ytterpunktene. Dernest kvalitetsmessig, fra å fokusere på utdaterte kompliserte problem, til komplekse problem som inkluderer stridsfeltets nye realiteter, inkludert cybermakt.

5 Avslutning

Cyberdomenet har en rekke egenskaper som fører med seg endringer og utfordringer som er pekt på i denne teksten. Spesielt er faktorene; more, mobility and mentality belyst. Disse faktorene fører til endrede maktstrukturer som videre har konsekvenser for organisering, og dernest lederskap av militære styrker. Det er vist til at cyberdomenet går på tvers av eksisterende domenene, samtidig som det krysser fysiske, kognitive og informasjons dimensjoner. Bevisst eller ubevisst motstand mot endring, eller evne og vilje til å ta innover seg eller forstå denne realiteten, gjør at nettverksbaseringen av Forsvaret har hatt redusert operativ effekt. Grunnen er at mennesker samhandler og kommuniserer for dårlig innenfor rammen av hierarkiet i en nettverksbasert realitet. Videre argumenteres det for at dette skyldes at maktstrukturer står i fare for å radikalt endres, og at dette dermed kan være en grunn til uvillighet til samhandling, kommunikasjon og nettverkstenking. Videre påpekes det at cyberdomenets inntog har konsekvenser for hvordan vi ser på lederskap konseptuelt, i praksis og i utdanning. Det er

vist til et eksempel der interne erfaringene gjort av FFI i det Norske Forsvaret og eksterne erfaringer gjort av McChrystal i interasjonale operasjoner påpeker samme utfordringer.

Utfordringene militære styrker står ovenfor i tiden fremover, krever at militære styrker organiseres annerledes. Det krever også at personellet tenker annerledes. I denne teksten argumenters det for at dette krever tilpasningsdyktighet foran størrelse og styrke, og at dette har store konsekvenser for lederskap. McChrystal har et godt poeng når han sier at: "There are few secrets to leadership. It is mostly just hard work." (McChrystal et al., 2016, s. 231). Og med dette i tankene, vil jeg påstå at det kreves mye hard tenkning og lite iverksetting for å få lederskap i Forsvaret inn på et fornuftig spor igjen.

6 Referanser

ACT. (2010). *NATO NEC Command and Control Maturity Model*. DoD Command and Control Research Program: Center for Advanced Concepts and Technology Retrieved from http://www.dodccrp.org/files/N2C2M2_web_optimized.pdf.

AJP_3-20. (Draft). *Allied Joint Doctrine for Cyber Operations*. Not Published: NATO.

Allen, S. H., & Machain, C. M. (2017). Understanding the impact of air power. *Conflict Management and Peace Science, 0*(0), 0738894216682485. doi:10.1177/0738894216682485

Andreassen, T. (2017). *The role of trust when implementing Network Based Defence in the Norwegian Armed Forces.* NTNU. Retrieved from http://daim.idi.ntnu.no/masteroppgaver/018/18079/masteroppgave.pdf

Aron, R. (1955). Europe and Air Power. *The ANNALS of the American Academy of Political and Social Science, 299*(1), 95-101. doi:10.1177/000271625529900112

Bibighaus, D. L. (2015). How Power-Laws Re-Write The Rules Of Cyber Warfare. *Journal of Strategic Security, 8*(4), 39-52. doi:http://dx.doi.org/10.5038/1944-0472.8.4.1439

Brangetto, P., & Veenendaal, M. A. (2016). *Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations.* Paper presented at the 8th International Conference on Cyber Conflct, Tallinn.

Buchler, N., Fitzhugh, S. M., Marusich, L. R., Ungvarsky, D. M., Lebiere, C., & Gonzalez, C. (2016). Mission Command in the Age of Network-Enabled Operations: Social Network Analysis of Information Sharing and Situation Awareness. *Frontiers in Psychology, 7*(937). doi:10.3389/fpsyg.2016.00937

Busch, T., Vanebo, O. V., & Dehlin, E. (2010). *Organisasjon og organisering* (6 ed.). Oslo: Universitetsforlaget.

FD. (2014). *Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren.* Retrieved from

https://www.regjeringen.no/globalassets/upload/fd/dokumenter/fdsretningslinjercyberoperasjoner.pdf.
FFI. (2016). *Støtte til Forsvarets NbF-utvikling-sluttrapport*. Retrieved from https://www.ffi.no/no/Rapporter/15-02403.pdf
FFOD. (2007). *Forsvarets Fellesoperative Doktrine*. Oslo: Forsvarsstaben Retrieved from https://brage.bibsys.no/xmlui//bitstream/handle/11250/99256/1/FFOD.pdf.
FFOD. (2014). *Forsvarets Fellesoperative Doktrine*. Oslo: Forsvarsstaben Retrieved from https://brage.bibsys.no/xmlui//bitstream/handle/11250/99256/1/FFOD.pdf.
Forsvaret. (2012). *Forsvarssjefens grunnsyn på ledelse*. Oslo: Sjef Forsvarsstaben.
Gibney, A. (Writer) & M. S. Alex Gibney (Director). (2016). Zero Days. In M. S. Alex Gibney (Producer).
Haaster, J. v. (2016). *Assessing Cyber Power*. Paper presented at the 8th International Conference on Cyber Conflct, Tallinn.
Høiback, H. (2017). Drømmen om Scharnhorst – om meningers mot. *PACEM, 20*(1), 31-42.
Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research, 1*(1), 80.
Johnsen, R. (2013). Cyberkrigføring og Forsvarets operative evne. *Internasjonal Politikk, 71*(02), 241-251 ER.
Jøsok, Ø., Knox, B. J., Helkala, K., Lugo, R. G., Sutterlin, S., & Ward, P. (2016). *Exploring the Hybrid Space Theoretical Framework Applying Cognitive Science in Military Cyberspace Operations.* Paper presented at the 10th International Conference, AC 2016, Held as Part of HCI International 2016, Toronto, ON, Canada.
Luktvasslimo, O. J. (2013). *Ledelse og lederutvikling i Forsvaret. Status og veivalg.*, Bedriftsøkonomisk institutt, Oslo. Retrieved from https://www.regjeringen.no/contentassets/09faceca099c4b8bac85ca8495e12d2d/no/pdfs/nou201620160008000dddpdfs.pdf
Lund, M. S. (2017). Cyber som operasjonsdomene. *Norsk Militært Tidsskrift, 186*(1), 28-34.
McChrystal, S. (2011). It takes a network. The new frontline of modern warfare. Retrieved from http://foreignpolicy.com/2011/02/21/it-takes-a-network/
McChrystal, S., Collins, T., Silverman, D., & Fussell, C. (2016). *Teams of teams: New rules of engagement for a complex world.* New York: Penguin.
MoD. (2013). *Finland's Cyber Security Straregy*. Helsinki: Secretariat of the Security Committee Retrieved from https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf.
Naím, M. (2013). *The end of power.* New York: Basic Books.
NATO. (2016). Warsaw Summit Communiqué. [Press release]. Retrieved from http://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en

NATO. (2017). Cooperative Cyber Defence Centre of Excellence. Retrieved from https://ccdcoe.org/cyber-definitions.html

Naughton, J. (2017). North Korea's deadliest weapon? Its hackers. *The Guardian*. Retrieved from https://www.theguardian.com/commentisfree/2017/oct/22/north-korea-deadliest-weapon-cyber-operations-sony-pictures?CMP=share_btn_link

NC3A. (2005). *NATO NETWORK ENABLED CAPABILITY FEASIBILITY STUDY*. NATO Retrieved from http://www.dodccrp.org/files/nnec_fs_executive_summary_2.0_nu.pdf.

NOU. (2016). *En god alliert - Norge i Afghanistan 2001–2014*. Oslo Retrieved from https://www.regjeringen.no/contentassets/09faceca099c4b8bac85ca8495e12d2d/no/pdfs/nou201620160008000dddpdfs.pdf.

Perkins, D. G. (2017). Multi-Domain Batte

Driving Change to Win in the Future. *Military Review*. Retrieved from http://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20170831_PERKINS_Multi-domain_Battle.pdf

Stortingsmelding. (2013). *Kompetanse for en ny tid*. regjeringen.no Retrieved from https://www.regjeringen.no/contentassets/16eb33bcb4b847509f9f7b28f7cfbefa/no/pdfs/stm201220130014000dddpdfs.pdf.

Stortingsproposisjon, S. (2016). *Kampkraft og bærekraft*. regjeringen.no Retrieved from https://www.regjeringen.no/contentassets/a712fb233b2542af8df07e2628b3386d/no/pdfs/prp201520160151000dddpdfs.pdf.

Strand, T. (2007). *Ledelse, organisasjon og kultur*. (2. utgave ed.). Bergen: Fagbokforlaget.

Strengen, M. (2014). *Virker krigsskoleutdanningen? Norske kadetters personlighetsutvikling gjennom tre år med offisersutdannelse.* (Master of Science), Forsvarets Høgskole, Oslo. Retrieved from https://brage.bibsys.no/xmlui/handle/11250/216611

Necesse 2018, Vol 3, Issue 2, 123-148 DOI: 10.21339/2464-353x.3.2.123

Fremtidens autonome ubemannede kapasiteter i Sjøforsvaret

Odd Sveinung Hareide, Sjøkrigsskolen/Navkomp
Tore Relling, IMPROVE/NTNU
Andre Pettersen, Forsvarets Forskningsinstitutt
Alexander Sauter, Sjøkrigsskolen
Frode Voll Mjelde, Sjøkrigsskolen/Navkomp
Runar Ostnes, NTNU
kontakt: oddsveinung.hareide@sksk.mil.no

Resyme. Sjøforsvaret har en lang historie med å utnytte ny teknologi for å øke den operative evne. Denne artikkelen tar sikte på å gi leseren økt forståelse av hva autonomi er, og hvordan dette kan nyttiggjøres i Sjøforsvaret. Sjøforsvarets intensjon med autonomi bør i hovedsak baseres på å redusere risiko for tap av menneskeliv, samt effektivisering av operasjoner der mennesket er en restriksjon. Begrepet autonomi blir gjort rede for, med fokus på de ulike gradene av automatisering samt utviklingen innen maritim autonomi. Videre gjøres det kort rede for hvilke sensorer vi har tilgjengelig i dag, hvordan disse kan bidra til trygg autonomi, og hvorfor robust navigasjon er essensielt for å oppnå dette. Avslutningsvis vil det argumenteres for hvordan autonome systemer, i samspill med mennesket, kan anvendes for å dekke Sjøforsvarets fremtidige operative behov.

1 Innledning

Om ti år vil Sjøforsvarets bemannede mineryddingsfartøyer være klare for utskiftning. Disse skal ikke erstattes med nye bemannede løsninger, men av ubemannede og aller helst autonome systemer (1). Mennesker skal ut av de farlige minefeltene og observere på trygg avstand, mens maskinene/roboten gjør den farlige jobben med å rydde minene. Utviklingen av avanserte ubemannede systemer i Sjøforsvaret startet allerede for flere tiår siden, hvor Hugin, Sjøforsvarets autonome undervannsfartøy, er et resultat av et langvarig samarbeid mellom industri, forskningsmiljøer og Forsvaret. Hugin er i dag en del av Sjøforsvarets operative undervannsleveranse og demonstrerer på en meget god måte hvorledes slike farkoster nyttes til klarering av minefarlige områder. I

samarbeid med Forsvarets Forskningsinstitutt (FFI) utvikler Sjøforsvaret nå autonome overflatefartøy som skal samspille med undervannsfartøyer for å gjennomføre mineryddingen med mindre bemanning. En slik løsning vil trolig også være billigere for Sjøforsvaret da spesialbygde bemannede fartøy som kan ferdes i minefelt er veldig kostbare.

Dette betyr ikke at Sjøforsvaret skal kvitte seg med alle menneskene, men at man går mot et nytt konsept hvor mennesker og høyteknologiske enheter fungerer sammen i menneske-maskin team for å løse komplekse og farlige oppdrag. Innføring av autonome systemer har som mål, men kan ikke garantere, et lavere bemanningsbehov. Operativ tilgjengelighet i Forsvarets operasjoner krever en robust organisasjon med kvalifisert personell for operasjon, vedlikehold og logistikk som fungerer 24/7 over lengre tidsrom (2).

For Sjøforsvarets del er målet å redusere menneskelig tilstedeværelse på kapasiteten av to årsaker;

1. å redusere risiko for mennesket
2. at mennesket ikke skal være en restriksjon på operasjonen (utmattelse, sløvhet, behov for mat/drikke etc).

De to overnevnte punkt er bakgrunnen for utarbeidelse og innholdet i denne artikkelen, og må leses i denne konteksten.

Ubemannede systemer er ikke ny teknologi. Helt siden første verdenskrig har ubemannede systemer blitt brukt i militære sammenhenger, men da som fjernstyrte fartøy. Den raske utviklingen innen informasjons- og kommunikasjonsteknologi (IKT) har gjort det mulig å redusere bruken av kontinuerlig styring fra operatører. Alt digitaliseres, regnekraften i datamaskinene øker, og sensorene blir mindre, bedre og billigere. Sammen med de nye utviklingene innen kunstig intelligens muliggjør dette autonome ubemannede systemer.

På mange områder har militære behov, forskning og utvikling vært drivende for teknologisk utvikling, for eksempel utvikling av radar under andre verdenskrig. Slik er det ikke lenger innen IKT og autonome systemer (3). Den teknologiske utviklingen har de siste tiårene akselerert, og en ser i dag stadig mer avanserte systemer bli satt i drift. Teknologien er i hovedsak drevet frem av sivile kommersielle krefter. Militæret i USA, Russland og Kina investerer enorme summer i teknologi, men må likevel dra veksler på den sivile teknologien for å

henge med. En positiv konsekvens av dette er at avansert teknologi har blitt rimeligere og lettere tilgjengelig for alle, også kjent som Commercial Off The Shelf (COTS) produkter (4).

2 Automatisering og autonomi

Autonomi kommer fra det greske ordet «autos» (selv, egen) og «nomos» (lov, regel eller styre), og betyr delvis eller fullstendig selvstendighet, selvstyre eller selvbestemmelse (5). Det finnes ikke en felles definisjon for hva autonome systemer er, og det blandes ofte mellom automatiske, fjernstyrte og autonome systemer. I et fjernstyrt ubemannet system er operatøren fysisk skilt fra systemet, men utfører fremdeles styringen og tar alle beslutningene. Hvis systemet er automatisert vil det kunne operere på egenhånd i hele eller deler av oppdraget (6), men fortsatt ha operatører ombord for å gjøre deler av oppdraget. Handlingene systemet skal utføre i ulike situasjoner er da forhåndsprogrammert. Et autonomt system er adaptivt og kan tilpasse seg situasjonen (7). Det skal kunne håndtere uforutsette hendelser, og er fristilt fra mennesket i utførelsen av operasjonen. Systemet må til en viss grad forstå situasjonen og utføre en handling som er tilpasset situasjonen og oppdraget. Handlingsmønsteret er gjerne basert på maskinlæring med trening hvor maskinen har bygget et erfaringsgrunnlag (8).

Sheridan og Verplank (9) beskriver følgende ti grader av automatisering:

Nivå	Forklaring
1	ingen assistanse, mennesket tar alle beslutninger og systemet bare utfører
2	datamaskinen tilbyr en komplett oversikt over beslutningsalternativene
3	datamaskinen foreslår beslutningsalternativer
4	datamaskinen foreslår ett beslutningsalternativ, mennesket bestemmer om det skal utføres
5	datamaskinen utfører foreslått alternativ hvis godkjent av menneske
6	datamaskinen tillater mennesket veto i en begrenset tid før utførelse

7	datamaskinen utfører automatisk og informerer mennesket
8	datamaskinen utfører automatisk, informerer mennesket bare ved fore spørsel
9	datamaskinen utfører automatisk, informerer mennesket bare hvis pre programmert
10	datamaskinen bestemmer alt, uten menneskelig innblanding.

Tabell 1. Sheridan *og Verplanks nivå av automasjon* (9).

Med autonomi menes vanligvis en selvstendighet i beslutningssystemet og starter dermed på nivå 6, med full-autonomt drift ved nivå 10. I denne artikkelen benyttes begrepet autonomi i løsninger med høy grad av automatisering som gjør at en kan redusere eller fjerne bemanning på fartøyene.

2.1 Maritim autonomi

Norges regjering har en uttalt ambisjon om å være ledende innenfor teknologi i havrommet. Maritim21 strategien beskriver at «Autonomi, automatisering og fjernstyring gir stort potensial for å reduserte kostnader og sikrere operasjoner, og vil kunne gjøre sjøtransporten konkurransedyktig i helt nye segmenter. Nye teknologier og markeder gir også store muligheter og behov for å etablere nye forretningsmodeller» (10).

Det er i dag flere initiativ i Norge som konkretiserer dette, og flere aktører er samlet gjennom Norsk Forum for Autonome Fartøy (NFAS), som er en interessegruppe for personer og organisasjoner som er interessert i temaet autonome fartøy (11). Verdens første testområde for autonome fartøy er opprettet i Trondheimsfjorden, kjent som «Autonomiområde Trondheimsfjorden» (12). Andre initiativ er samarbeidet mellom Yara og Kongsberg for å realisere fartøyet «Yara Birkeland», som skal operere mellom Brevik og Larvik og erstatte 40 000 lastebilturer i året (13). I dette konkrete prosjektet ser en for seg en tre-stegs modell der fartøyet først er bemannet ett år (2018), videre fjernstyrt i ett år (2019), for til slutt å operere autonomt i løpet av 2020 (14).

Fig. 1. Autonomiprosjektet «Yara Birkeland» (kilde: https://www.tu.no/artikler/verdens-forste-autonome-fartøy-i-drift-skal-erstatte-40-000-vogntogturer-i-aret/382717)

NFAS har presentert et forslag til grader av maritim autonomi, vist i tabell 2 under.

Nivå	Operatørens rolle	Automatisering	Kompleksitet
0	Besetning på broen	Ingen: Direkte kontroll av menneske	Få statiske objekter
1	Tidvis ubemannet bro overvåket av kontrollstasjon på land som kan påkalle besetning	Veiledning til operatør, ingen automatisk kontroll	Mange statiske objekter
2	Ubemannet fartøy, kontinuerlig overvåket fra kontrollstasjon på land	Menneskelig tilsyn, automatisk og deterministisk kontroll ved bruk av enkle grenseverdier	Mer dynamisk miljø, ingen begrensninger på fartøyets manøvrerbarhet
3	Periodisk ubemannet bro	Automatisk og deterministisk	Forholdsvis dynamisk miljø,

	uten overvåkning fra kontrollstasjon. Systemet kan mønstre bemanningen på fartøyet ved behov.	system med lengre og mer komplekst beslutningssystem	noen begrensninger på fartøyets manøvrerbarhet.
4	Ubemannet med tilsyn fra kontrollstasjon, kontrollstasjon gir ordrer ved behov	Begrenset autonomi – flere men begrensete valgmuligheter for fartøyets beslutningssystem	Dynamisk miljø, noen begrensninger på fartøyets manøvrerbarhet
5	Ubemannet, ingen overvåkning fra kontrollstasjon på land	Fullt autonomt – ingen begrensninger på beslutningssystem	Dynamisk miljø, begrensninger på fartøyets manøvrerbarhet.

Tabell 2. Grader av autonomi i det maritime domenet, norsk oversettelse (15).

I tabell 2 vises sammenhengen mellom de fem ulike nivåene av maritim automatisering sammenstilt med operatør, automasjonsgrad og kompleksitet i operasjonen. Dette gir et bedre bilde på autonomi i det maritime domenet fra et mer økonomisk/industriell perspektiv.

Automatiseringen har startet for lenge siden, men det er først nå at teknologien begynner å bli moden for at fartøyene kan ha en mer helhetlig selvstendig kontroll. Norge kan bruke nasjonale regler innenfor 12 mils sonen, som for eksempel Yara Birkeland benytter seg av. Internasjonalt vil det fortsatt ta lang tid før en har en løsning på flere problemstillinger relatert til autonome fartøy, dette blant annet på grunn av tunge beslutningsprosesser i International Maritime Organization (IMO). Vi kommer til å se en gradvis innføring av mer og mer automatisering og mulighet for fjernstyring, før en overgang til fult autonome systemer vil skje. Teknologien for autonomi er i vesentlig grad tilstede, men det er nødvendig å ta et helhetlig systemperspektiv for å utvikle et

robust konsept. Det betyr at en må se på teknologi i samspill med menneskelige og organisatoriske faktorer (16).

3 Sjøforsvarets behov for autonomi

For å vurdere ubemannede overflatefartøy (Unmanned Surface Vehicle - USV) med mulighet for høyere grad av autonomi, må en se på sensor-, styre- og beslutningssystem samt kommunikasjonsbærere som muliggjørende teknologi (Figur 2).

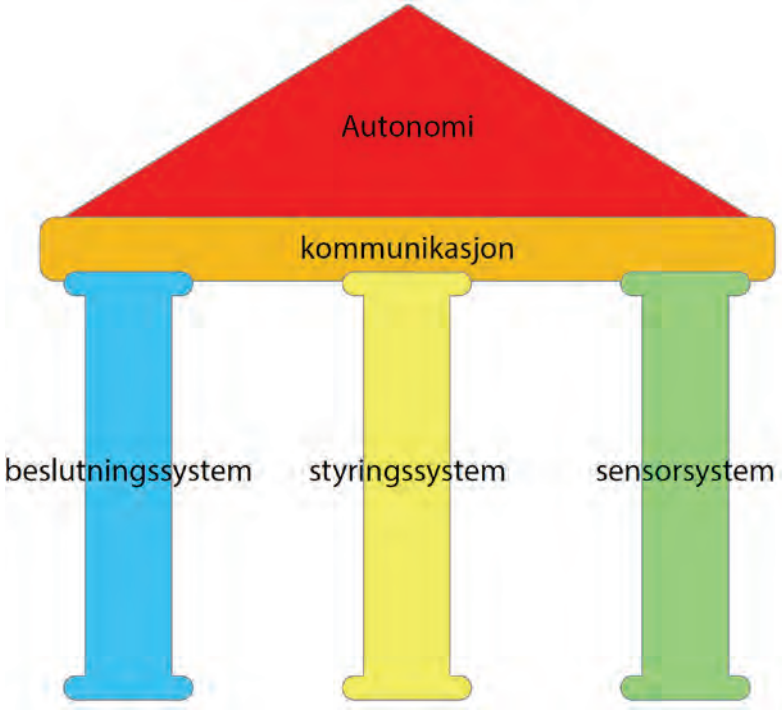


Fig. 2. Bærebjelker for realisering av autonomi

3.1 Robust navigasjon

Robust navigasjon er evnen til å kunne navigere trygt og sikkert til enhver tid under alle forhold. I et autonomt system generelt, og for militær bruk spesielt, er det viktig med et system som er designet med både høy grad av redundans og robusthet i styrings-, kommunikasjon- og sensorsystem. Redundans kan eksemplifiseres med samtidig bruk av GPS og Galileo GNSS. Om én skulle

bortfalle eller være feilaktig så kan den andre brukes eller feilen oppdages. Robusthet i sensorinformasjonen betyr at en benytter komplimenterende teknologier som kan belyse situasjonsbildet fra flere sider. Et eksempel er bruk av terrengnavigasjon der en sammenligner data med GNSS, for å sikre fartøyets posisjon, men også for eksempel for å oppdage (uventede) endringer i terrenget. Med bemannede fartøy er mennesket en viktig del av denne robustheten i navigasjonen, mens på autonome fartøy må robusthet designes inn i systemet.

Med å benytte seg av sensorene som er tilgjengelige, kan en få informasjon om fartøyets absolutte eller relative posisjon, samt informasjon om fartøyets bevegelser (fart og retning). En kan utnytte radar (relativ posisjonering – korrelasjon mot kart) for mer robust navigasjon. Videre kan terrengnavigasjon, ved for eksempel bruk av undervannstopografien, utnyttes for å øke robustheten til systemet (17).

Måten som de fleste aktører tenker å gjennomføre posisjonering, samt utføre måloppdagelse og unngå kollisjon på, er å benytte en rekke forskjellige, gjerne (delvis) redundante sensorer (for eksempel bruk av både S-band, X-band og CW Radar), for å skape et tilstrekkelig godt situasjonsbilde til å ta målrettede beslutninger. Den romlige overlappen i sensormålingene er eksemplifisert i Figur 3.

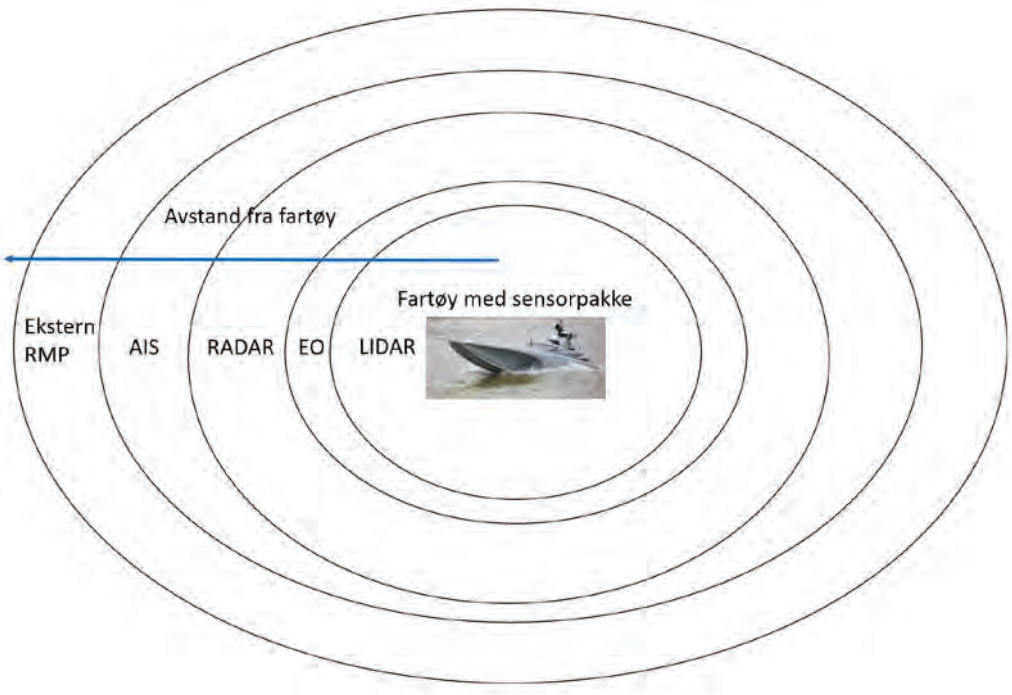


Fig. 3**.** Måloppdagelse med ulike sensorer i autonomi, figuren er ikke uttømmende.

3.1.1 Kommunikasjon

Kommunikasjon mellom fartøy og land (kommando og kontroll) kan være utfordrende, og det er prøvd ut ulike løsninger for å håndtere dette med hensyn på utveksling av data og størrelsene på datapakkene. Løsningen kan være å bruke en sømløs overgang mellom alle de ulike kommunikasjonsbærerne for å tilfredsstille båndbredde samt holde kostnader nede. Det er også utfordringer i forhold til størrelse på datapakkene som det er behov for å sende, på tross av nye komprimeringsteknikker. Med flere sensorer vil det også følge økende mengde data. Sammen med en kommunikasjonsbærer kommer også muligheter og begrensninger innenfor maritim datasikkerhet (18, 19), som er et økt fokusområde både sivilt og militært, spesielt med hensyn på den siste tids hendelser med skadevare og ransomware (for eksempel WannaCry og Stuxnet) (20). Maritim Bredbåndsradio (MBR) er installert på flere av Sjøforsvarets fartøy, og er også utprøvd i operativ tjeneste med gode resultater. Dette er et eksempel på en løsning som kan være med på å bidra til større båndbredde, mer robusthet og sikrere dataoverføring (21). I et fullt autonomt system vil det kunne

gjennomføres et oppdrag over en lengre periode uten noen form for kommunikasjon, et eksempel på dette er Hugin AUV (22). Hugin blir pre-programmert før deployering, og kan gjennomføre mine-mottiltak (MCM), vurderinger av miljøet (Rapid Environmental Assessment – REA) og etterretningsinnsamling, overvåkning og rekognoseringsoppdrag (ISR). Dette uten behov for kommunikasjon mens oppdraget pågår. En kan derfor argumentere med at behovet for robust kommunikasjon mellom fartøyet og kommandoinstansen blir mindre ved innføring av fullt autonome fartøy, som ikke har samme kommunikasjonsbehov som fjernstyrte og semi-autonome fartøy.

I en militær kontekst så er robusthet en av faktorene for suksess, dette er ytterligere fremhevet av at navigasjonskrigføring er introdusert som en krigføringsgren i NATO. I krise, konflikt eller krig vet vi at det vil være begrenset mulighet for å benytte seg av systemer som kan påvirkes utenifra. Dette har senest blitt bekreftet ved signalforstyrrelser/jamming av GNSS i Øst-Finnmark og Svartehavet (23, 24). Robust navigasjon blir derfor sett på som en suksessfaktor for å benytte seg av autonomi, spesielt i en militær kontekst.

3.1.2 Styresystem

Styresystemet er bindeleddet mellom sensor-input på den ene siden, og aksjonene som utføres på den andre siden. Tradisjonelt vil store deler av hva som skal skje bli bestemt av mennesket, men f.eks. automatiske sikkerhetsprotokoller kan være implementert allerede på et lavt nivå av automatisering. Sikkerhetsprotokoller overstyrer når mennesket gjør «gale» avgjørelser, men kan også overta når styresignalene uteblir, for eksempel ved å kjøre motorene kontrollert ned. «Styresystemet» kan i navigasjonssammenheng tolkes som utelukkende navigasjonsstyrende. I dette tilfelle vil da f.eks. retning og fart/pådrag være de direkte utgangene som styres. I videre og mer overordnet forstand kan derimot «styresystemet» tolkes som alt som har med styring om bord å gjøre, all informasjon fra hver sensor og motor og opp til kontrollskjermen vil da være dekket. Sentralt i dette signal-nettverket er vanligvis Programmerbare Logiske Styringer (PLSer), som normalt fungerer i en hierarkisk oppbygning og styrer delsystemene etter fast definerte regler. Kombinasjonen av inngangssignalene, både fra sensorer og via brukergrensesnitt, sammen med noe form for minne av hva som har skjedd tidligere, vil da entydig bestemme utgangssignalene. I sin enkleste form kan det

bety at lyset går på om bryteren slås på, men av igjen etter en definert tid. Ved overgang til autonomi vil da den delen av inngangsinformasjonen som består av signaler fra kontrollrommet/mennesket overtas av at annet beslutningssystem. PLSer forblir ofte som bindeleddet mellom beslutnings-, styrings og sensorsystemene. Om hvor vidt delsystemene i et fullt autonomt fartøy fremdeles vil ha egne uavhengige styringsoppgaver, muligens med faste sikkerhetsprotokoller som kan overstyre systemet på samme måte som for manuell styring, er uvisst. Maskinlæring og kunstig intelligens (AI) kan ha nytte av å få rådataene fra alle delsystemene. Sannsynligvis vil det, i hvert fall i startfasen, være mest naturlig å implementere delsystemer som stort sett fungerer uavhengige, som da integreres hierarkisk i nye AI-nivå. Uansett, så forventes det at styresystemet vil vokse nærmere sammen med beslutningssystemet i autonome fartøy. Enn så lenge er intelligente systemer som er i stand til å utføre komplekse styringsavgjørelser separert fra den klassiske styringen som underligger på klassisk PLS-nivå.

3.2 Autonomt beslutningssystem[1]

I et helautonomt system hvor operatøren er erstattet av datamaskiner, er det viktig å presisere at autonomibegrepet er relativt. Dette fordi den autonome kapasiteten vil være en del av et overordnet system, med en overordnet målsetning, og det er dette overordnete systemets målsetning som avgjør om det autonome systemet får tildelt et oppdrag og hvordan oppdraget er formulert. Derfor er det autonome systemet kun autonomt innen de gitte rammene for oppdraget, men fremdeles underlagt et overordnet system som kan ha en annen grad av automatisering. Når et oppdrag er gitt må fartøyet selv tolke og planlegge hvordan oppdraget best kan løses, og gjennomføre det selvstendig. Hvis noe skulle skje underveis som påvirker gjennomføringen eller graden av måloppnåelse, må fartøyet re-planlegge eller avbryte oppdraget.

Et autonomt system består av noen standard funksjonaliteter. Disse er mer eller mindre avanserte avhengig av kompleksiteten i oppdragene og miljøet fartøyet skal operere i, samt hvilken tilpasningsevne som er nødvendig. Kjernen i autonomien er et beslutningssystem som kan ta avgjørelser og prioritere, basert

[1] Denne delen er utarbeidet basert på erfaringer fra FFIs arbeid innenfor maritime autonomi til og med ut 2017.

på informasjon og et rasjonale som ligger i programvaren. Systemet må både kunne planlegge frem i tid for å løse oppdraget, samt kunne reagere på oppdukkende hendelser og informasjon underveis. Tilsvarende som for en operatør trenger også maskinen informasjon for å kunne planlegge og reagere. Noe av informasjonen er forkunnskap; hvilke sensorer, funksjoner og ytelse har fartøyet, samt hvilke kartgrunnlag som er tilgjengelig for området, er eksempler på dette. Annen informasjon må samles inn underveis ved hjelp av sensorer. Denne informasjonen kan sammenliknes med bruk av sansene til en operatør for å observere omgivelsene og for å forstå fartøyets tilstand.

Det er helt avgjørende for et autonomt system å samle inn informasjon om omgivelsene. Det er denne informasjonen som gjør fartøyet i stand til å tilpasse seg omgivelsene og løse oppdragene, og dette kaller vi for sceneanalyse og er vist i Figur 4.

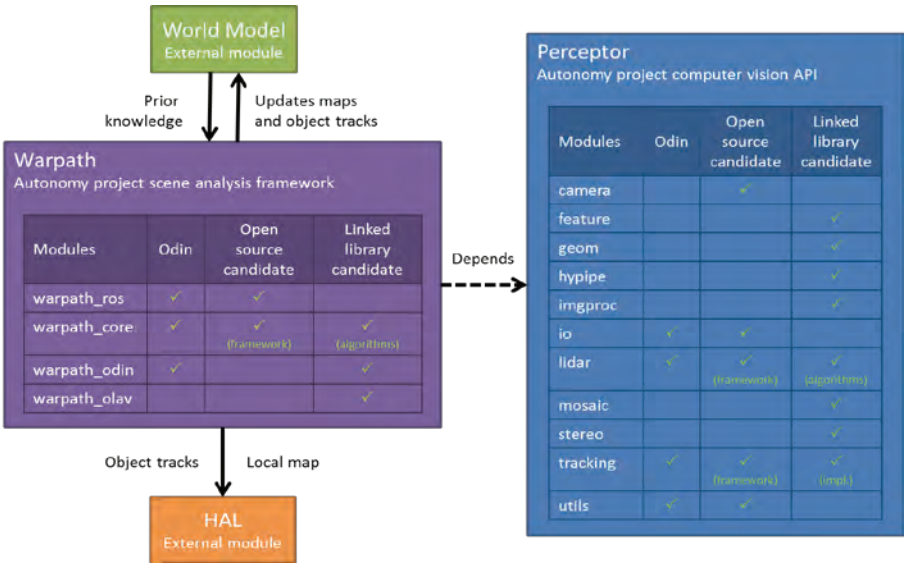


Fig. 4. Sceneanalyse (kilde: FFI)

Fartøyet må ha et sett av sensorer som gir robust og utfyllende informasjon om omgivelsene. Hvilke sensorer som er nødvendig er avhengig av miljøet og oppdraget. Målet er at fartøyet skal kunne bedømme fremkommelighet, forstå vesentligheter i omgivelsene, identifisere objekter, posisjonere seg selv, navigere og ikke minst samle informasjon nødvendig for å løse oppdraget. Forskjellige

typer radarer med ulike frekvenser, laserskannere, kameraer, sonarer, mikrofoner, ultralyd og Electronic Support Measures (ESM) er eksempler på sensorer som kan brukes. Generelt vil mange ulike sensorer gi et bedre og mer robust bilde av omgivelsene. Sensordata bør også fusjoneres på tvers av ulike (komplementerende) sensorer, og de bør samspille i undersøkelsen av omgivelsene for å trekke ut mest mulig informasjon. Fartøyet setter sammen den innsamlede informasjonen i en modell av den nåværende omkringliggende verden. En slik modell blir en kombinasjon av forinformasjon (eksempelvis kart), informasjon sendt til fartøyet og egne observasjoner prosessert om bord (Hybrid Autonomy Layer – HAL) (25).

En viktig del av sceneanalysen er å finne, spore (tracke) og gjenkjenne objekter. Fartøyet må kunne klassifisere hva de ser, og ofte også identifisere. I en militær sammenheng kan det bety å klassifisere og identifisere motstanderens militærfartøy. Det er tatt store steg innen kunstig intelligens og bildegjenkjenning, og maskiner er i dag på høyde med mennesker når det gjelder gjenkjenning. Spesielt har utviklingen innen dyp læring, der dataalgoritmene etterlikner nevronene i hjernen, gitt gode resultater. Gjenkjenningsalgoritmene kan også brukes til GNSS-uavhengig posisjonering og navigasjon. Hvis fartøyet eksempelvis gjenkjenner et sjømerke og posisjonen til merket er kjent, vet også fartøyet sin posisjon. Dette er teknikker som allerede demonstreres på fartøy i dag. Maskinene kan også finne og velge kjennemerker automatisk, og lage egne lokale kart og utføre relativ posisjonering. Dermed kan et autonomt fartøy lære og utvikle seg til å bli bedre over tid.

Sivile og militære teknologier for autonomi er stort sett like i fremgangsmåten for sceneanalyse, men militære fartøy vil ha større utfordringer på grunn av kravene til robusthet. Fartøyet må i mange sammenhenger operere skjult og en motstander vil prøve å hindre kommunikasjon og posisjonering av fartøyet i varierende grad. En konsekvens er at det er økt behov for at systemene må kunne operere autonomt i perioder uten kontakt med en operatør, samt uten bruk av sårbare delsystemer (for eksempel kommunikasjonsbærer). Det er også perioder der aktiv utsendelse av signaler vil avsløre posisjonen til fartøyet, regulert av Emisson Control (EMCON). I et oppdrag med streng EMCON vil sceneanalyse med utelukkende passive sensorer være nødvendig. Systemene må også være uavhengig av GNSS på grunn av trusselen fra navigasjonskrigføring. I henhold til dagens trusselbilde vet en at GNSS ikke vil være tilgjengelig i en krise,

krig eller konflikt, og fartøyet må derfor bruke andre sensorer for å posisjonere seg og navigere trygt og effektivt (19).

Sceneanalyse gir informasjon om den ytre verden, men fartøyet må også samle informasjon om egen tilstand og ytelse. Oppstår feil i systemene må konsekvensen og eventuelle tiltak vurderes. Kan oppdraget likevel løses helt eller delvis, eller må fartøyet avbryte og returnere, eventuelt starte en nødprosedyre? I dette ligger det at fartøyet må kjenne sin egen ytelse og hvordan feil eller endringer vil påvirke fartøyets evne og mulighet til å gjennomføre oppdrag i den pågående operasjon. Det trenger heller ikke å være kritiske tekniske feil som oppstår, men for eksempel kan noen av sensorene få redusert ytelse. Dette kan skyldes miljøforhold som regn eller tåke. Tilsvarende som med en operatør om bord må da fartøyet justere sensorparametere, og eventuelt endre hvilke sensorer som legges vekt på i sceneanalysen.

Beslutningene som tas må basere seg på tilgjengelig informasjon og et rasjonale. Mange beslutninger, som å unngå statiske og dynamiske hindringer, krever utregninger, men vanligvis ikke kunstig intelligens - AI. Planlegging av ruter som holder fartøyet skjult, finner raskeste vei, utnytter værforhold eller alle kriteriene samtidig handler om optimalisering av komplekse problemstillinger. Ved beslutninger om feilhåndtering med påfølgende vurdering og justering av ytelse, må maskinen sette informasjonen inn i en større helhet, og vurdere konsekvenser og måloppnåelse samt vurdere kvalitet i sensordata. Når alt skal settes i sammenheng til et velfungerende system som skal løse et oppdrag blir dette komplisert. Spesielt hvis oppdraget, miljøet og en motstanders mottiltak øker kompleksiteten. Det vil stilles store krav til fartøyets evne til autonomi, og blant annet maskinlæring kan bidra til å løse dette.

Maskinlæring er et felt i sterk utvikling. I en slik læringsprosess opparbeider maskinene erfaring gjennom eksperimentering. Maskiner kan da trenes til å løse komplekse oppgaver, så lenge systemet kan trenes i det. Med enkel automatisering vet vi stort sett hendelsene som kan oppstå, og vi kan fortelle maskinen hvordan hendelsene/utfordringene skal løses. Blir situasjonen vanskelig å forutsi må maskinene utforske et mye større løsningsrom, samt håndtere uforutsette hendelser, noe som er typiske problemstillinger ved autonome systemer. Maskinlæring er ikke uproblematisk. Maskinene blir ikke bedre enn den treningen de utsettes for, og en måte å overføre menneskers kunnskap til de autonome systemene er at mennesker er veiledere. Situasjoner spilles av og mennesker gir innspill til løsninger og tilbakemelding om resultater.

Det er tidskrevende og det er en viss fare for at menneskelige feil overføres til maskinen. En annen måte er at maskinene trenes gjennom simuleringer eller datasett, der mange scenarier utforskes, og maskinene forsøker å optimalisere utfallet. Dagens dataprosesseringskapasitet muliggjør store mengder simuleringer, og muligheten/evnen til læring for datamaskiner blir derfor akselerert. På tross av dette er (mangelen på) kvalitet og mengden av treningsdata hovedutfordringen. Dette vil naturligvis bli enklere når de første autonome systemene er i operativ drift og samler data til skolering av neste generasjons systemer.

3.3 Behov i Sjøforsvaret

Sjøforsvaret består i dag av fregatter, korvetter, ubåter, minefartøy, kystvaktfartøy, stridsbåter samt en del mindre fartøy (26). Det er signal i Langtidsplan for Forsvaret at antallet større fartøy vil reduseres i fremtiden (27), blant annet gjennom utfasing av korvettene og en reduksjon i antall ubåter i forhold til dagens antall.

I Sjøforsvarets strategiske konsept utredes det operative konseptet med en tilpasset landorganisasjon for å kunne videreføre Sjøforsvaret på lengre sikt på en hensiktsmessig måte, med de oppdrag som fortløpende blir gitt (1). Sjøforsvaret har identifisert teknologi som et av satsningsområdene, herunder ubemannede systemer og automatisering. Det poengteres at operativ anvendelse av ubemannede systemer kan forbedre situasjonsforståelsen, redusere menneskelig arbeidsbelastning, og minimere faren for tap og skade på sivilt og militært personell (2). Sjøforsvarets strategiske konsept er godt forankret sett i sammenheng med øvrige allierte nasjoners doktriner, samt teorier for maritim anvendelse av droner til bruk i operasjoner som kjennetegnes av å være kjedelig, skitne eller farlige (Dull, Dirty, Dangerous – DDD). Sjøforsvarets strategiske konsept mener at automasjon kan øke operativ evne gjennom forbedret overvåkning, responsevne, forbedret kommunikasjon og koordinasjonsevne, økt tilstedeværelse og reduksjon i driftsavbrudd (1).

Det anbefales videre en helhetlig satsning på de definerte teknologiområdene for å utvikle et moderne Sjøforsvar som skaper balanse i bredde og dybde (1).

3.4 Menneske-system integrasjon

Anskaffelse og innføring av ny teknologi i Forsvaret må være styrt av en tilnærming hvor brukerforutsetningene er sentrale i utformingen av menneske-maskin-systemer. Brukere av moderne våpensystemer forventer produkter som kan brukes trygt og effektivt.

Teknologisk utvikling gir Forsvaret muligheter til å ta i bruk systemer med mindre eller større grad av autonomi i den hensikt å kunne løse nåværende og fremtidige oppdrag på en best mulig måte. Innføring av autonome systemer vil påvirke taktikk og konsepter i et fremtidig forsvar, og usikkerheter i forhold til en kombinasjon av bemannede og ubemannede systemer må synliggjøres og analyseres.

Tabell 3 viser noen av utfordringene som må løses for at ubemannede systemer, som er i interaksjon med mennesker, skal bli en styrkemultiplikator for dagens og femtidens sjøforsvar (2, 28, 29).

Operatør utfordringer	Beskrivelse
Redusert sanseinntrykk	Operatøren av en ubemannet farkost har begrenset utendørs visning for å hjelpe med navigasjon, kollisjonsunngåelse og observasjon av vær og omgivelsesfaktorer. Fraværet av hørsel, lukt og inntrykk av bevegelse kan også gjøre det vanskeligere å overvåke tilstanden til fartøyet. Ombordkameraer, der hvor disse er tilgjengelig, kan gi operatøren et ensidig bilde som kun dekker et begrenset synsfelt.
Kontroll og kommunikasjon	Operatøren må kunne overvåke kvaliteten på kommando-, og kontrollsignaler med enheten. Radioforstyrrelser, dataforsinkelser og utfordringer med datasikkerhet kan gjøre direkte kontroll vanskelig.
Konstruksjon av kontrollstasjon	Kontrollstasjoner ligner mer og mer på et kontrollrom eller et kontor enn en tradisjonell operatørposisjon som man finner på bemannede systemer. Romsligheten i mange kontrollstasjoner

	gjør det enkelt å montere ytterligere skjermer og systemer uten fokus på optimal plassering. Dette kan gjøre det vanskelig å håndheve faste eller naturlige ombordprosedyrer.
Overføring av kontroll under pågående operasjoner	Kontroll av en ubemannet farkost kan overføres under pågående operasjoner mellom tilstøtende kontrollkonsoller, innenfor en kontrollstasjon eller mellom geografisk adskilte stasjoner. Hver overføring kan innebære en risiko for signalfeil, motstridende kontrollinnstillinger eller feilkommunikasjon.
Svikt i situasjonsbevissthet	Det er utfordrende å opprettholde tilstrekkelig aktsomhetsnivå på langvarige operasjoner, selv på bemannede enheter. Ekstern monitorering av ubemannede systemer medfører ytterligere fravær av impulser, noe som kan redusere operatørens oppmerksomhet og dermed evnen til å opprettholde situasjonsbevissthet (SA).
Tillit til automasjon ved høy grad av autonomi	Anvendelse av ubemannede enheter med høy grad av autonomi krever at man har tillit til automasjon for manøvrering og operering. Det kan være en tillitsutfordring for mennesker å samhandle med teknologisk avanserte enheter som de ikke selv kan kontrollere.
Bemanning	Et ubemannet system krever fortsatt mennesker, til tross for utbredte krav/forventninger om at autonomi vil redusere personellbehovet. Det må gjennomføres grundige analyser for å belyse faktiske behov. Her må krav til utholdenhet og utførelse i tiltenkte operasjonsmønstre tas med i betraktning slik at posisjoner som krever bemanning har tilstrekkelig antall personell med nødvendig kompetanse og trening.

	Høy grad av operativ tilgjengelighet krever samtidig gode støttefunksjoner for vedlikehold og logistikk.

Tabell 3. Noen utfordringer innen menneske-maskin integrasjon

Undersøkelser gjennomført av det amerikanske luftforsvaret analyserte forekomsten av UAV-uhell i alle forsvarsgrener i perioden 1995-2005 (30). Rapporten viste at ulykkesfrekvensen for UAV var høyere enn for konvensjonelle fly, og at menneskelige faktorer innen organisasjon, operasjon eller vedlikehold var medvirkende eller direkte årsak til 68% av UAV-uhell. Kombinert med en rapport fra NASA (31) ble betydelige bidragsytere til UAV-uhell identifisert som: Utilstrekkelig erfaringsnivå på UAV-operatører og vedlikeholdspersonell, utilfredsstillende nivå på seleksjon av UAV-operatører, trening og treningskriterier, for mange forskjellige UAV-systemer, komplekse menneske-maskinmiljøer, dårlig design av kontrollstasjon, manglende standarder og retningslinjer, samt mangel på dokumentasjon, prosedyrer og sjekklister.

Fokus på integrasjonen mellom mennesket og systemet vil (29)

- optimalisere operativ evne
- begrense feilhandlinger og øke systemets overlevelsesevne
- sikre interoperabilitet
- redusere behov for bemanning og trening
- balansere bredde og dybde i strukturen
- redusere livssykluskostnader (LCC)

Behovet for integrasjon tidlig i innkjøp og anskaffelse av menneske-maskin systemer kommer klart til syne i utforming av brukervennlige grensesnitt mellom operatør og utstyr. En tommelfingerregel for HMI (Human Machine Interface) brukervennlighet er 1: 10: 100 (29). Hvis det koster 1x å fikse et problem under design, vil det koste 10x når systemet er utviklet, og 100x når det er operativt. Med andre ord er avkastningene store ved tidlig integrasjon (32).

Systemets totale prestasjon avhenger av en helhetlig integrasjon av det menneskelige element i design, anskaffelse og drift av komplekse teknologier og systemer (33). Forståelsen av grunnleggende forutsetninger for menneskelige prestasjoner og anvendelsen av denne kunnskapen i design og integrasjon av ny

teknologi er avgjørende for optimal operativ ytelse, og dette gjelder også for Forsvaret (29).

3.5 Kommando og kontroll av autonome kapasiteter

Ved å endre til et konsept med kapasiteter som er ubemannede vil en ha behov for å utøve lederskap på en annen måte enn i dag. Forsvarets doktrine for maritime operasjoner beskriver både hvordan oppdragsbasert ledelsesfilosofi og nettverksbasert forsvar skal benyttes for å nå overordnet målsetning (34). Begge disse krever en tett interaksjon mellom nivået som har kommando og kapasiteten som skal utøve oppdraget.

I oppdragsbasert ledelse er gjennomføring av sjefens intensjon essensielt, der en delegerer valg av handlemåte. Men det krever også at en skal kommunisere hvordan en velger å løse oppdrag tilbake til den som har gitt oppdraget. Det er også viktig å ta hensyn til at oppdragsbasert ledelse ikke utelukker at høyere enhet ønsker å detaljstyre operasjoner, og den teknologiske utviklingen har ført til at en oftere både har mulighet og ønske om å kontrollere operasjonene høyere i kommandokjeden enn tidligere. Spesielt i krisesituasjoner og tidlig i en konfliktsituasjon, hvor den politiske føringen kan være å unngå en eskalering, vil sentralisert ledelse være viktig. Nettverksbasert forsvar som konsept fjerner seg vekk fra å tenke på den enkelte plattform, og har som mål å muliggjøre et koordinert samvirke og konsentrasjon av effekt (34). Forsvarets doktrine er dermed i stor grad avhengig av interaksjoner mellom kapasiteter, og mellom kapasitet og kommandomyndighet. Disse interaksjonene vil være annerledes når mennesket ikke opererer kapasiteten og en må finne andre måter å etablere disse interaksjonene på. Det mest nærliggende er at en benytter mennesker til å kontrollere kapasitetene og selv om kapasiteten har et høyt nivå av autonomi, vil systemet inkludert kommando og kontrollapparatet totalt sett kunne ha et lavt nivå av autonomi, og dermed vurderes mer som en fjernstyrt operasjon.

Fjernstyrte operasjoner er ikke noe nytt, og ved at en opererer fartøyet fra land gir det mulighet til å utøve kommando og kontroll på tradisjonell måte. Dette kan også gi fordeler ved at de som kontrollerer farkostene kan lokaliseres nært kommandomyndighet, og dermed kunne bedre interagere mellom det utøvende ledd og beslutningstagere. Dette både fordi samlokalisering er mulig, men også fordi sensorer som er nødvendig for operasjon samtidig vil gi et godt situasjonsbilde for en beslutningstager. Utfordringen ved å utøve fjernstyrte

operasjoner er godt kjent blant annet fra bruk av droner, og spesielt bør en ta hensyn til det menneskelige aspektet ved å være langt unna operasjonen som kan gi utfordringer for operatørene (35, 36).

Det er vesentlig at det tas en diskusjon om hva ubemannede kapasiteter vil bety for kommando og kontroll. Ved en høy grad av autonomi ligger det til grunn at systemene selv skal ta beslutninger om handlemåte. Dersom de militære kapasitetene skal operere uavhengig av kontekst (fredstid, krisesituasjon eller krig) så vil det være mindre utfordrende enn dersom konteksten skal bygges inn i autonomien. I fred og krise vil en så langt det lar seg gjøre ha sentralisert kontroll, og desentralisert utøvelse. Det vil si at en ikke ønsker å delegere beslutningsmyndigheten ned til fartøynivå. I en krigssituasjon, hvor en ofte kan tenke seg at det er et mer avklart fiendebilde, kan en derimot se for seg at mer autonome løsninger kan være aktuelle. Likevel er en avhengig av samvirke med andre kapasiteter for å konsentrere effekt, og denne interaksjonen og vurdering om når og hvor denne konsentrerte effekten skal skje kan være en utfordring å bygge inn i en autonom løsning. Det er viktig i videre utvikling av ubemannede kapasiteter at en tar hensyn til at mennesket også i fremtiden vil utøve kommando og kontroll over kapasiteten. Dette betyr at en må kunne ha mulighet til å kommunisere med kapasiteten, samt kunne tolke hva kapasiteten har lagt til grunn for sine beslutninger.

3.6 Kompetanse innenfor autonomi

Med innføring av høyere grad av autonomi kommer også behovet for riktig kompetanse for personellet i den spisse ende (operatøren). «Riktig kompetanse» forstås slik at både teknisk og operativt personell får tilført den kompetansepakken som er nødvendig for å øke forståelsen, slik at en kan benytte seg av autonomien på en hensiktsmessig måte med hensikt til å øke operativ evne. Det er også viktig å poengtere viktigheten av gode relasjoner mellom forskningsmiljøer og operative enheter, dette for å hindre et gap mellom det akademiske miljø som utvikler de autonome systemene og den operative virkeligheten (37).

Det har den siste tiden vært økt bruk av teknologi, kanskje spesielt når det kommer til operasjonalisering. Flere sensorer og system som før var forbeholdt spesial operasjoner er nå blitt kommersielt tilgjengelige, noe som medfører et økt kompetansepress på sluttbrukeren (operatøren/navigatøren). Utfordringen

kan da være at en har avansert teknologi tilgjengelig, men at en ikke har personell til å benytte/forstå det (illustrert i Figur 5). Det er derfor essensielt at en beholder kompetente mennesker som en del av systemet, selv i en autonom kontekst (38).

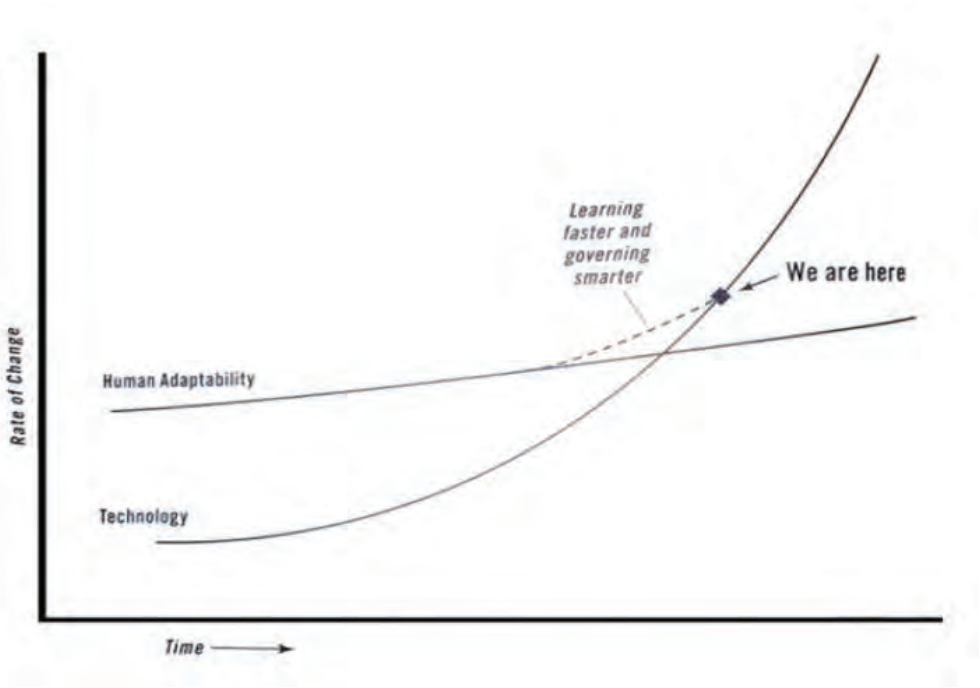


Fig. 5. The Knowing/Doing Gap (Eric Teller, CEO of Google X)

Samtidig argumenteres det for at autonomi vil være «intuitiv» og dermed enklere å bruke. Det vil si at autonome systemer ikke nødvendigvis krever økt kompetanse. Autonomien skal senke brukerterskelen og systemene skal i stor grad være selvstendige. Det vil da være et spørsmål om det krever endret kompetanse, og hvilken type endret kompetanse i form av lavere eller høyere kompetansekrav. Dette kan være i form av større forståelse av teknologi, samtidig som en må bruke mennesker til det de er gode til. Kompetansen innenfor maritim autonomi krever mer forskning, og det eneste som er sikkert er at dette vil føre til et paradigmeskift for den maritime navigatøren.

3.7 Operasjonelle konsept for Sjøforsvaret

Flere operasjonelle konsept er allerede identifisert og iverksatt gjennom Sjøforsvarets operative konsept og FFIs prosjekter. Spesielt innenfor minemottiltak er Sjøforsvaret godt i rute.

Eksempler på operasjoner der autonome overflatefartøy (Autonomous Surface Vessel – ASV) og bruk av maritime droner vil antas å bidra til økt operativ evne:

1. Maritim overvåkning

For å opprette og vedlikeholde et maritimt overflatebilde (RMP) vil ASVer fungere som mobile sensorstasjoner som kan holde oversikt over et begrenset geografisk område over en gitt tid. Kvaliteten og tiden ASVen kan gjøre dette begrenses av sensorer, høyde på sensorene, samt type drivstoff og hvor mye drivstoff det er plass til. Ved maritim overvåkning kan en forvente potensielt store mengder data, noe som kan være en utfordring.

2. Målangivelse

ASV benyttes for tredjeparts målangivelse (TPT), samt bidra til målangivelse over horisonten (OTHT) til andre plattformer med egnet våpenlast, for eksempel Naval Strike Missile (NSM). Her kan en også se for seg muligheten for at ASVen ligger i «dvale» i lengre perioder, for så å bli aktivert ved behov.

3. Styrkebeskyttelse

Styrkebeskyttelse, for eksempel av utenlandske fartøy som besøker havner i Norge, er et oppdrag som Sjøforsvaret må utføre. Dette er gjennomført med ulike plattformer, men i hovedsak utføres det av mindre plattformer under 20 meter. Her er flere konsept allerede prøvd ut, og det eksisterer kommersielle løsninger (COTS) til dette formålet.

4. Logistikk

I konseptet Maritime Combat, Service and Support (MarCSS), brukes mindre enheter for å understøtte deler av logistikken. Dette kan ASV/USVer også gjennomføre på en effektiv måte.

5. Maritime droneteam

Etablere og benytte maritime droneteam i gjennomføring av operasjon. Droneteamene består av teknisk og operativt personell som kan gjennomføre en konvertering av eksisterende fartøy til høyere grad av autonomi for bedre å løse

et relevant oppdrag. For eksempel kan en tenke seg en modularitet, der både autonomipakke og effektorer for å løse et oppdrag (sensorer, system og/eventuelt våpen) medbringes av droneteamet til en egnet plattform. Droneteam kan være embarkert på større enheter, og benytte seg av eksisterende plattformer langs kysten som en form for moderne og teknologisk sjøheimevern.

4 Konklusjon

Sjøforsvaret har identifisert og iverksatt en økt satsning innenfor autonomi, i den hensikt å redusere risiko for tap av menneskeliv, samt gjennomføre en effektivisering av operasjoner der mennesket fremstår som en restriksjon. Automatisering kan ses på som en del av autonomi utviklingen, og med dagens sensorer og system er det allerede tilrettelagt for høy grad av autonomi. Den største utfordringen ligger innenfor autonome beslutningssystemer for å kunne oppnå en høyere grad av autonomi. Dette blir det per dags dato jobbet målrettet med, og det er flere konkrete prosjekter på gang i Norge. Det vil bidra til å skape mer kunnskap, og i enda større grad operasjonalisere det maritime autonome konseptet.

Muliggjørende teknologi for økt grad av autonomi består av sensorer, kommunikasjonsbærere, styresystem og beslutningssystem. Sensorer genererer data, og autonomien skapes når data automatisk prosesseres om bord og informasjonen som trekkes ut behandles av et beslutningssystem som handler selvstendig på bakgrunn av de data som er tilgjengelig. Sammenstilling eller fusjon av alle de ulike sensordataene og forhåndskunnskap som sjøkart, og betydningen av denne informasjonens innhold, er da et vesentlig punkt for å realisere autonomi. Kommando og kontroll vil være utfordrende og krever mer kunnskap, samt at menneske-maskin interaksjonen i ubemannede og autonome systemer må anerkjennes som en utfordring og håndteres deretter.

Områder som maritim overvåkning, målangivelse, styrkebeskyttelse, logistikk og maritime droneteam er eksempler på operative konsepter der økt grad av autonomi kan være med å bidra til økt operativ evne. For FFI og annen sivil norsk industri er maritim autonomi et satsningsområde, og Norge har en uttalt strategi om å være ledende innenfor det maritime autonome domenet. Det er derfor viktig at Sjøforsvaret fortsetter med målrettet forsknings- og utviklingsarbeid

innenfor autonomi for å utnytte synergier. Det bør utredes flere konsept for å utforske mulighetsrommet ved utnyttelsen av autonomi i Sjøforsvaret.

5 Referanseliste

1. Sjøforsvarsstaben. Sjøforsvarets Strategiske Konsept, 2016-2040. Bergen2014.
2. DoD U. Unmanned systems integrated roadmap: FY2013-2038. Washington, DC, USA. 2013.
3. Page RM. The early history of radar. Proceedings of the IRE. 1962;50(5):1232-6.
4. Iversen SE. Militær navigasjon basert på Commercial Off The Shelf (COTS) produkter. Necesse. 2016;1(1).
5. Leksikon SN. Autonomi 2014 [Available from: https://snl.no/autonomi.
6. Lee JD, Sanquist TF. 17 Maritime Automation. Automation and Human Performance: Theory and Applications. 2018:220.
7. Schiaretti M, Chen L, Negenborn RR, editors. Survey on autonomous surface vessels: Part I-a new detailed definition of autonomy levels. International Conference on Computational Logistics; 2017: Springer.
8. Batalden B-M, Leikanger P, Wide P, editors. Towards autonomous maritime operations. Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA), 2017 IEEE International Conference on; 2017: IEEE.
9. Sheridan TB, Verplank WL. Human and computer control of undersea teleoperators. Massachusetts Inst of Tech Cambridge Man-Machine Systems Lab; 1978.
10. Strategigruppen. Maritim21-strategi. In: fiskeridepartementet N-o, editor. Bergen2016.
11. NFAS. Norsk Forum for Autonome Skip 2016 [Available from: http://nfas.autonomous-ship.org/.
12. Sjøfartsdirektoratet. Åpner verdens første testområde for autonome skip 2016 [Available from: https://www.sjofartsdir.no/aktuelt/nyheter/apner-for-test-av-autonome-skip/.
13. Stensvold T. Verdens første autonome skip i drift skal erstatte 40.000 vogntogturer i året. Teknisk Ukeblad. 2017.
14. Kongsberg. YARA and KONGSBERG enter into partnership to build world's first autonomous and zero emissions ship 2017 [Available from: https://www.km.kongsberg.com/ks/web/nokbg0238.nsf/AllWeb/98A8C576AEFC85AFC125811A0037F6C4?OpenDocument.
15. NFAS. Definition of autonomy levels for merchant ships. Trondheim; 2017.
16. Boy G. Orchestrating human-centered design: Springer Science & Business Media; 2012.
17. FFI. Terrengreferert posisjonering for undervannsfarkoster Kjeller: FFI; 2001. Report No.: FFI/RAPPORT-2001/05900

18. Fitton O, Prince D, Germond B, Lacy M. The future of maritime cyber security. Lancaster University; 2015.
19. Hareide OS, Jøsok Ø, Lund MS, Ostnes R, Heikala K. Enhancing Navigator Competence by Demonstrating Maritime Cyber Security. Journal of Navigation. 2018;71(5).
20. Schröder-Hinrichs J-U, Praetorius G, Graziano A, Kataria A, Baldauf M, editors. Introducing the Concept of Resilience into Maritime Safety. 6th Symposium on Resilience Engineering, Lisbon, Portugal, June 22-25, 2015; 2016: Resilience Engineering Association.
21. Kongsberg. Maritime Broadband Radio 2016 [Available from: https://www.km.kongsberg.com/ks/web/nokbg0240.nsf/AllWeb/BCCBAC3EA4EA6785C1257E280039BD63?OpenDocument.
22. Marthiniussen R, Vestgard K, Klepaker RA, Storkersen N, editors. HUGIN-AUV concept and operational experiences to date. Oceans -04 MTTS/IEEE Techno-Ocean -04; 2004 9-12 Nov. 2004.
23. Goward D. Mass GPS Spoofing Attack in Black Sea?2017 10.08.17. Available from: http://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea.
24. NRK. Støy fra Russland slo ut GPS-signaler for norske fly2017. Available from: https://www.nrk.no/finnmark/stoy-fra-russland-slo-ut-gps-signaler-for-norske-fly-1.13720305.
25. FFI. Fra butikkjøpte droner til 24-timers robotpatrulje 2016 [Available from: http://2016.ffi.no/sverm.
26. Forsvaret. Sjøforsvaret 2017 [Available from: https://forsvaret.no/sjoforsvaret.
27. Forsvarsdepartementet. Kampkraft og bærekraft - Langtidsplan for forsvarssektoren Oslo2016.
28. Hobbs A, Lyall B. Human Factors Guidelines for Unmanned Aircraft System Ground Control Stations. NASA. 2015.
29. Mjelde FV. Oppnåelse av Forsvarets oppgaver gjennom teknologisk integrasjon. Necesse. 2016;1(1):46-9.
30. Tvaryanas AP, Thompson WT, Constable SH. US military unmanned aerial vehicle mishaps: Assessment of the role of human factors using human factors analysis and classification system (HFACS). Human Systems Wing (311th) Brroks AFBTX; 2005.
31. Hobbs A, Herwitz SR. Human Challenges in the Maintenance of Unmanned Aircraft Systems. FAA and NASA Report. 2006.
32. Pressman RS. Software engineering: a practitioner's approach: Palgrave Macmillan; 2005.
33. Booher HR. Handbook of human systems integration: John Wiley & Sons; 2003.
34. Forsvaret. Forsvarets doktrine for maritime operasjone. In: Forsvarsstaben, editor. Bergen: Sjøfrosvarsstaben; 2015.
35. Chappelle WL, McDonald KD, Prince L, Goodman T, Ray-Sannerud BN, Thompson W. Symptoms of psychological distress and post-traumatic stress disorder in United States Air Force “drone” operators. Military medicine. 2014;179(8S):63-70.

36. Prince L, Chappelle WL, McDonald KD, Goodman T, Cowper S, Thompson W. Reassessment of psychological distress and post-traumatic stress disorder in United States Air Force distributed common ground system operators. Military medicine. 2015;180(3S):171-8.
37. Hareide OS, Vågenes S. Operativ FoU - et eksempel. Necesse. 2017;2(1):5.
38. Hukkelås T. Autonomi i havrommet. GCE Node; Grimstad2017.

Necesse 2018, Vol 3, Issue 2, 149-163 DOI: 10.21339/2464-353x.3.2.149

An Attack on an Integrated Navigation System

Mass Soldal Lund[1], Odd Sveinung Hareide[2,3], and Øyvind Jøsok[1,4]

[1] Norwegian Defence University College, Cyber Academy
[2] Norwegian Defence University College, Royal Norwegian Naval Academy, Navigation Competence Center
[3] Norwegian University of Science and Technology, Joint Research Program in Nautical Operations
[4] Inland Norway University of Applied Sciences, Faculty of Social and Health Sciences

Abstract. Maritime cyber security is emerging as a field as reports of cyber attacks against computerized maritime systems have started arriving. Modern vessels are equipped with computerized systems for navigation employing the Global Positioning System (GPS), known as Integrated Navigation Systems (INS) and Electronic Chart Display and Information Systems (ECDIS). This paper describes a proof-of-concept attack on an INS and its integrated ECDIS, and reports on a demonstration of the attack on a vessel. The attack includes malware that acts as a man-in-the-middle intercepting and manipulating GPS coordinates. Furthermore, the paper discusses the feasibility of the attack, as well as countermeasures.

Keywords: Cyber security · Integrated Navigation System · ECDIS

1 Introduction

Maritime cyber security is emerging as a potentially large concern [8,9,13,33]. Modern vessels are equipped with computerized systems for navigation using Global Navigation Satellite Systems (GNSS) such at the Global Positioning System (GPS). Lately, reports of cyber attacks against maritime systems have started arriving and have placed cyber security at sea on the agenda [4,7]. One type of attack is GPS spoofing, in which navigation systems are fooled by the transmission of false GPS signals [24,30]. In a recent incident, more than 20 vessels operating in the Black Sea reported receiving obviously wrong GPS positions in what appears to be a massive GPS spoofing [14].

Maritime navigation systems connected through onboard networks are usually referred to as Integrated Navigation Systems (INS) [20]. In an INS, operator stations with software for displaying the vessel's position in electronic charts – known as Electronic Chart Display and Information Systems (ECDIS) [19] – are integrated with the GPS and other devices such as heading sensors (gyroscope), depth sensors, Automatic Identification System (AIS), etc. [16] (see Fig. 1).

In order to build defenses, it is necessary to understand attacks. In this paper we report on a proof-of-concept attack on an INS, and the practical demonstration of the attack conducted on a vessel in cooperation with the Royal Norwegian Navy (RNoN).[1]

The main feature of the attack is to infect the ECDIS software on an operator station with malware that acts as a man-in-the-middle intercepting and manipulating incoming coordinates from the GPS. This can be seen as a kind of GPS spoofing that does not interfere with the signals of the GPS satellites, but with the internal signaling of the INS. In addition the malware can crash the operator station by provoking a bluescreen. The system on which the attack was demonstrated is air-gapped, i.e. without an Internet connection; a USB Human Interface Device (HID) attack is therefore used for delivery. The attack is rather crude, but we believe that it demonstrates the feasibility of this kind of attacks. To some degree, the attack depends on bad security of maritime systems. Several reports available indicate that there are large cyber security challenges in the maritime sector (see e.g. [4,7,10,26]). Such reports are usually produced by security companies, which may have an interest in exaggerating the situation, but on the other hand we should also expect underreporting of incidents. In the absence of more systematic studies the overall state of cyber security at sea is unknown. The attack presented in this paper nonetheless highlights the need for maritime cyber security, and also what can be gained (security wise) from implementing relatively simple security measures.

The remainder of the paper is organized as follows: We first give a brief presentation of the INS in question and some of its main features (Section 2). This is followed by a detailed presentation of the attack and its development, structured after the intrusion kill chain model of Hutchins et al. [17], including a report from the practical demonstration of the attack [15] (Section 3). After presenting the attack, we discuss possible further developments (Section 4), as well as the feasibility of the attack and possible counter-measures (Section 5). Finally, we provide conclusions (Section 6).

2 Integrated Navigation System (INS)

The INS in question, illustrated in Fig. 1, is a network that connects a number of operator stations (bridge consoles) with the sensors of the vessel. The diagram shows the sensors, such as the Global Positioning System, the Gyro System, the Automatic Identification System and so forth, connected to a sensor integrator (SINT) through serial connections (blue lines). The operator stations are connected to the same SINT through switches in a Dual LAN (red lines). The Dual LAN is two parallel Ethernets of which one is a backup, thus providing redundancy. As a second redundancy feature, the operator stations also have serial connections to the SINT (thin blue lines). The role of the

[1] The INS and ECDIS in question are anonymized per request of the provider. The owner of the vessel and the provider of its INS supported the project and had representatives participating in the planning, the reconnaissance and the practical demonstration. The provider of the INS has been offered all information concerning the attack and has approved of the publication of this paper.

SINT is to receive signals from the sensors and communicate them to the operator stations in a common format, thus providing a single source of sensor data. In addition the SINT integrates an autopilot (AP). The operator stations are regular desktop computers running ECDIS software on top of the Windows operating system. The ECDIS software interprets the signals received form the SINT and uses information such as GPS coordinates and AIS messages to render the vessel's position and heading, as well as the position of nearby vessels, in the chart.

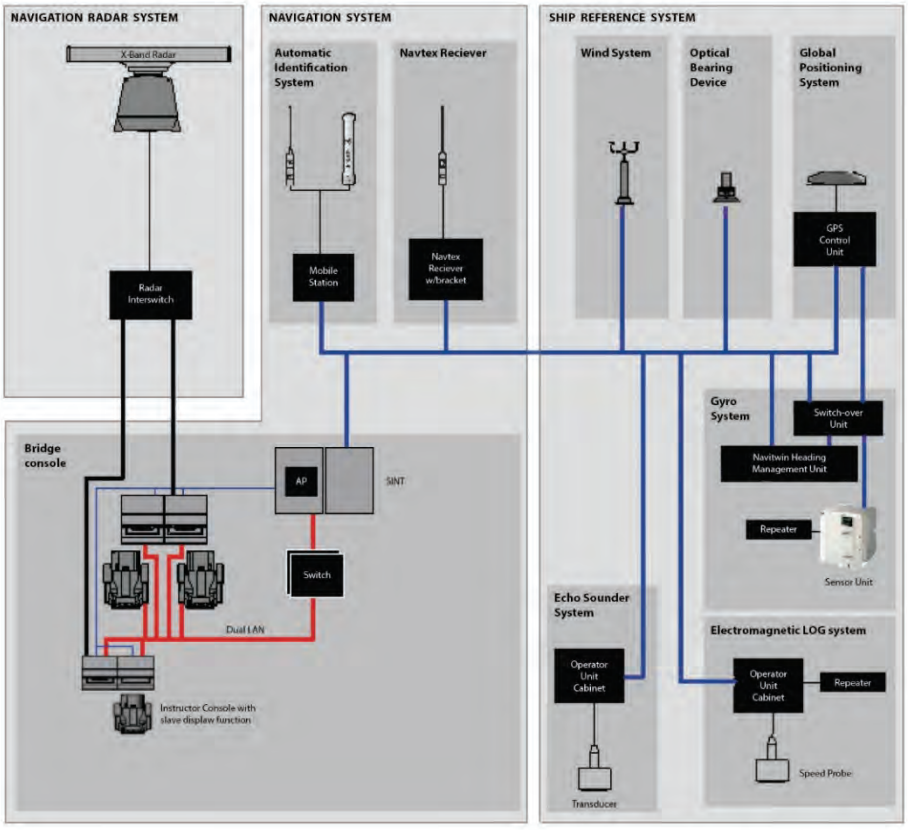


Fig. 1. Schematic of the INS from the vessel's documentation (courtesy of RNoN)

3 Attack

The intrusion kill chain [17] is a tool developed for analyzing cyber attacks. It provides a model that describes the work process of an attacker seeking to infiltrate computer system in seven phases: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. Thus, while the model is developed as an aid to the defender it utilized the waypoint of the attacker. This makes it a good tool also for describing the development of an attack, because it will highlight

the assumptions and choices made, and the resources needed, in the development. In the following we explain our attack in detail according to the seven phases of the intrusion kill chain. At the end of the section we report from a demonstration of the attack.

3.1 Reconnaissance

In our reconnaissance efforts, we had four main sources of information:

1. A field trip was conducted on board a vessel identical to the vessel on which the demonstration was to take place. During this field trip we observed the workings of the system and had the opportunity to ask questions to representatives of the owner of the vessel and the provider of the INS.
2. During the field trip, we also had the opportunity to monitor and capture data traffic on the INS network while the vessel was sailing. This was achieved simply by plugging a regular laptop computer with Wireshark installed into a spare port in the switch using a network cable.
3. We obtained a laptop with the ECDIS software installed.
4. We were given access to technical documentation of the INS installation of the vessels.

In addition, some testing and troubleshooting was performed on a second field trip when the attack was demonstrated. The likelihood of an attacker being able to perform the same kind of reconnaissance is discussed in Section 5.1.

From the field trip we learned that operator stations are running Windows 7 and logged in with user profiles with administrator privileges. Inspection of the ECDIS software on the laptop we obtained showed that it uses Windows Sockets 2.0 (Winsock) for network communication. Inspection of its configuration files, held together with the documentation, gave useful information about the configuration of the network, e.g. that all nodes have static IP addresses. This, together with the network traffic capture, also told us the IP addresses of the network and port numbers used in the communication. Analysis of the network traffic capture revealed the format of the SINT signals, which turned out to be User Datagram Protocol (UDP) multicasts of plaintext messages formatted according to the NMEA 0183 standard, usually referred to as NMEA sentences. For learning the details of NMEA sentences we used more or less arbitrary Internet source [5,36].

3.2 Weaponization

The payload of the attack consists of two parts: a fake Windows socket dynamic-link library (Winsock DLL) and a script that crashes the computer by provoking a bluescreen. The fake Winsock DLL is a proxy for the proper Winsock DLL (`ws2_32.dll`) developed using available skeleton code [2]. It acts as a man-in-the-middle between the proper DLL and the ECDIS software, inspecting and manipulating data packages received from the network. The SINT transmits the NMEA sentences as ASCII plaintext; an NMEA sentence with GPS coordinates is of the following format:

```
$GPGGA,083548.53,6022.10378,N,00510.06015,E,1,11,0.8,
  54.74,M,,M,,*71
```

The letter code at the start (`GPGGA`) identifies the sentence as one carrying a GPS position. Identifying and changing the coordinate (60°22.10' N, 5°10.06' E) is straightforward; the ECDIS software will accept a modified sentence as long as the checksum at the end (`*71` in the example) is recalculated.

The other part of the payload is a script that causes a bluescreen. It utilizes the PsKill application of the Windows Sysinternals package [32] to kill an essential system process (the Client/Server Runtime Subsystem, `csrss.exe`). The script itself is written in VBScript, as are all other scripts used in the attack. The reason for this choice (as opposed to using for example PowerShell) is to make the attack compatible with basic installations of both Windows XP and Windows 7 as both Windows versions are commonly used as platforms for ECDIS applications [10,23,25].

Crucial for the development of the payload was the setup of a test environment. We used VMware software to virtualize the laptop with the ECDIS software installed and put it in a virtual network with a simple SINT simulator – a Debian VM running a small Python script generating UDP multicasts containing NMEA sentences with GPS coordinates.

3.3 Delivery

For delivery of the payload we made a device consisting of a Teensy microcontroller [29], a USB flash drive and a USB hub. Utilizing the possibility of programming the Teensy microcontroller to simulate a USB keyboard and a USB mouse at the same time, we developed a so-called USB HID attack (see e.g. [28]). The delivery is in three phase:

1. The ECDIS software has a built in key capturing feature that prevents keyboard shortcuts (such as Windows key + `R` to get the Windows Run dialog) from being effective. This is circumvented by simulating keyboard and mouse to enter a maintenance password which allows this feature to be disabled. (Some considerations on the passwords of the system are made in Section 5.1.)
2. With the key capturing feature disabled, the simulated keyboard uses keyboard shortcuts to open a command prompt. In the command prompt it uses command line tools to make necessary changes to the computer, as well as to type, save and run a small script.
3. The script identifies the USB flash drive and obtains the payload from it.

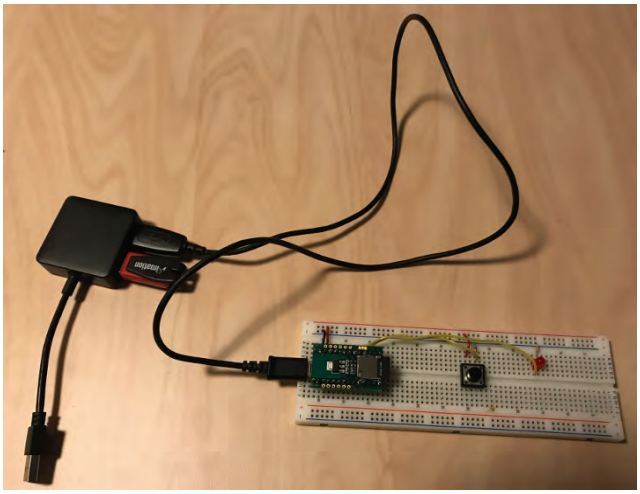


Fig. 2. Prototype USB delivery device consisting of a Teensy microcontroller, a USB flash drive and a USB hub

The choice for this means of delivery was based on the assumption that the INS is air-gapped. Thus, it was necessary with a method based on some form of physical access. Using simulated keyboard and mouse have the benefit that we do not need to assume an exploitable vulnerability in the operating system or other software. Furthermore, we could not rely on downloading the payload through the Internet. Having the simulated keyboard type the whole payload would take an unacceptable amount of time. (In a test, the simulated keyboard needed approximately seven and a half minutes to type a Base64 encoding of the 161 kB payload.) To avoid this, the choice fell on combining the Teensy with a USB flash drive though a USB hub. The (prototype) device is shown in Fig. 2.

The scenario for application of this means of delivery would be for the attacker to discretely insert the device into a USB socket on one of the operator stations during a visit on the bridge of a vessel. Other means of delivery that we believe may work are discussed in Section 4.1.

3.4 Exploitation

The attack does not exploit technical vulnerabilities in the operating system or other software. The vulnerabilities exploited in the delivery is the fact that the target computer by default is logged in with a user profile with administrator privileges, combined with physical access and knowledge of the maintenance password of the ECDIS software. The attack itself exploits the possibility of tricking the ECDIS software into loading the fake Winsock DLL in what is sometimes called a DLL search order hijacking attack (see e.g. [12]).

3.5 Installation

A common way of installing malware is to first deliver a small program or script which downloads the main payload via an Internet connection, a so-called dropper. However, we worked under the assumption that the target system is air-gapped. In the attack we therefore have the simulated keyboard deliver the dropper – by typing, saving and executing a script – and then have the dropper copy the payload – a zip file – from the USB flash drive to the hard drive of the target computer and unzipping it. A combination of keystrokes from the simulated keyboard and scripts contained in the payload then accomplishes the installation: The fake Winsock DLL is copied to the installation folder of the ECDIS software, and the registry of the computer is updated to exclude Winsock from KnownDLLs in order to trick the software into loading the fake DLL. (KnownDLLs is a mechanism for ensuring that certain standard DLLs are loaded from the Windows distribution, see e.g. [12].) In addition, a scheduled task is created that runs a script for provoking bluescreens. (The bluescreen script is described in more detail in Section 3.7). Finally, the computer is restarted to make the changes come into effect; the default user profile is automatically logged in and the ECDIS application launched on startup. In the demonstration of the attack (see Section 3.8) the time used by the full delivery and installation was 5 minutes, 17 seconds, including restart of the computer and the ECDIS software which took 2 minutes, 26 seconds. This means the time used by the USB device was 2 minutes, 51 seconds, but there is a potential for optimizing the process. We believe the time used by this first part (i.e. the time the USB device has to remain in the USB socket) can be reduced by approximately one and a half minutes. The installation is visible, but one option for preventing this could be to have the device dim the screen as its first action.

3.6 Command and Control

As the target system is air-gapped, the attack does not rely on any command and control mechanisms. However, in Section 4.2 we discuss a possibility of devising a simple form of command and control without violating the assumption that the system is air-gapped.

3.7 Actions on Objectives

When installed, the attack can perform two kinds of actions: It can manipulate GPS coordinates received from the SINT via the network and it can provoke the operator station to crash with a bluescreen. The manipulation of GPS coordinates is performed by adding a small accumulating (positive or negative) deviation to the latitude, longitude or both, each time an NMEA sentence carrying GPS coordinates is received. A bluescreen, as mentioned above, is provoked by the killing of an essential system process.

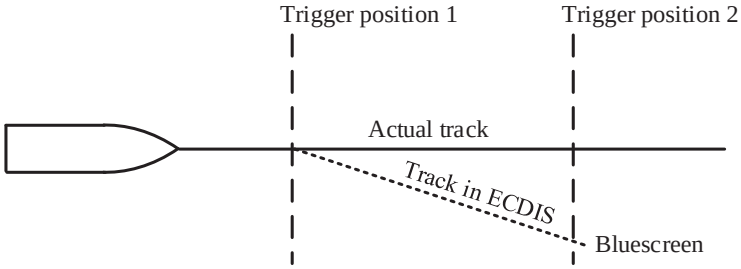


Fig. 3. Illustration of test run during the demonstration

Both actions are triggered by the position of the vessel. The intercepted GPS coordinates are compared to a set of specified triggering conditions, essentially rectangles defined by northern, southern, eastern and western limits. In the case of the GPS manipulation, the deviation will grow with a specified value every time a new GPS coordinate is received (approximately twice each second) as long as the received coordinates are within the specified limits. Outside of the limits the deviation will still be added to the coordinates, but as a constant. In the case of the bluescreen, a file is written to the hard drive of the computer if the triggering conditions are met. A script running every minute (activated by a scheduled task) checks the presence of the file, and if the file exists performs the process kill that provokes the bluescreen.

3.8 Demonstration

Both parts of the attack, as well as the delivery, were successfully demonstrated in four test runs during a passage in the littoral waters outside of Bergen, Norway in late August 2017. The vessel is equipped with several operator stations (see Fig. 1); by infecting one of them with the malware we could compare an infected and an uninfected operator station during the test runs. A typical test run is illustrated in Fig. 3. We specified two trigger positions. At the first trigger position the malware started accumulating the deviation, and thus the position shown in the ECDIS software started drifting from the actual track. At the second triggering position the malware provoked a bluescreen which made the operation station crash.

Fig. 4. Route plotted by ECDIS software using GPS data. Uninfected operator station to the left, infected operator station to the right

Fig. 4 shows the route plotted by the GPS in one of the test runs (in which the bluescreen was not tested) – uninfected operator station to the left and infected operator station to the right. In this test run the deviation grew by approximately 0.8 m toward north and 0.4 m toward east per second.

4 Further Development

The attack as implemented utilizes a specific vector of delivery and has no command and control structure. Both are in a sense features of the attack that are separate from its core, which is the manipulation of GPS data. In this section we examine how the attack may be developed further by using other means of delivery or by implementing a command and control structure.

4.1 Delivery

Our means of delivery was a special USB device that in any realistic scenario must be brought wittingly to the bridge of the vessel under attack by an agent. However, it should be worth considering other methods of delivery that do not have this requirement. The most obvious would be to make a malware that can spread via USB flash drives. For example, a case in which an ECDIS computer on board a large tanker was infected by malware when charts were updated using an infected USB flash drive has been reported [4]. Another obvious option would be to utilize an Internet connection. We developed the attack for a vessel on which the network is air-gapped, and traditionally such systems have been air-gapped due to lack of good Internet connections at sea. This is however changing, and navigation systems are now increasingly being equipped with Internet connections over satellite and/or 4G broadband (for use when sailing close

to shore) [4,7,10,25]. Furthermore, it has been demonstrated how this can be exploited to launch attacks [10,34].

A perhaps less obvious attack vector can be illustrated by tests we did during our reconnaissance when we plugged a laptop computer into the switch of the INS. This possibility is a common feature since stand-alone laptops are often used to plan routes, which are later transferred to the operator stations using the network. We were able to communicate (using e.g. Ping and nmap) with the other computers in the network after assigning our laptop a static IP address in the range used by the network. Clearly, there is a potential for using an external computer plugged to the network as a vector for delivery. Similarly, there would be a potential for the malware to spread between operator stations connected to the network.

4.2 Command and Control

In the attack we used the reception of specific GPS coordinates as a trigger for the malware to perform certain actions. However, we could easily have used any other information transmitted on the network by the SINT as the triggering condition. In our virtual test environment, we have demonstrated how the Automatic Identification System (AIS) can be used to develop a simple kind of command and control. AIS is an automated tracking system used extensively in the maritime world for exchange of information for anti-collision purposes. Ships and land-based stations equipped with AIS transceivers broadcast AIS messages containing static information (identity, vessel type, etc.) as well as voyage related (destination) and dynamic information (position, heading, speed) using the VHF spectrum [27]. As illustrated in Fig. 1, the INS integrates AIS. The ECDIS software of the operator stations receives AIS messages from the SINT and renders information from nearby ships in the navigation charts. An AIS message is basically a number of values packed in a bit string. This bit string is encoded as ASCII characters in a fashion similar to Base64 encoding and transmitted as part of an NMEA sentence [31]. We had the fake Winsock DLL inspect AIS messages received from the simulated SINT and use the reception of specific vessel names as the triggering condition. We also encoded encrypted commands into AIS messages to make the malware on an operator station trigger bluescreens, change its triggering conditions, write to the hard drive and execute commands. We believe that constructing an AIS transceiver to transmit such coded messages would be doable given moderate resources, see [3]. Furthermore, the AIS on the vessel gets certain kinds of information, e.g. the specified destination, from the ECDIS software via the network and the SINT. Even though it was not tested, we believe this can be exploited to have the malware make the AIS transmit simple messages, e.g. to acknowledge received commands. The downside of this means of command and control is the relatively low bitrate of AIS which makes transfer of large files or data unpractical. (AIS uses two channels each with a bit rate of 9.6 kbits/s, but due to overhead, data encoding and conflict resolution the practical transfer rate is at least an order of magnitude lower [21]).

As mentioned in the previous section, navigation systems with Internet connections are becoming more common. In addition to providing another vector for delivery, this obviously opens up for other methods of command and control.

5 Feasibility and Counter-Measures

The attack was made under certain assumptions; the feasibility of the attack obviously depends on their validity. In the following we discuss the feasibility of the attack in the view of these assumptions. First, however, it should be recognized that the attack was successfully tested on an INS installation on a vessel without any prior modification of the system to make the attack work. Furthermore, the attack did not exploit any known or unpatched vulnerabilities in the installation. This in itself should demonstrate that the attack is possible. The question of the feasibility of the attack is therefore a question of whether we had unreasonable good intelligence and access, and a question of the effectiveness of barriers and counter-measures and to what degree they are implemented. We will discuss these two questions in turn.

5.1 Reconnaissance

It cannot be denied that we were given an excellent opportunity with access to software, documentation, network traffic, a full installation and experts on the system. On the other hand, these systems are commercially available and any actor could get the same access given sufficient resources. It would certainly be achievable for a state actor or a large criminal organization. The only piece of information used in the attack that we would not be able to obtain by buying an installation of the system is the maintenance password used to bypass the key capturing functionality. How easy it would be to obtain this password illegitimately will of course be speculation. The use of shared or role based passwords, as well as relying on access control implemented at the application level rather than the operating system, are considered security challenges in the context of industrial control systems (SCADA systems) [22]; these worries should carry over to navigation systems. However, research on password use suggests that password mechanisms should reflect the nature of the resources protected in order to avoid undermining the mechanism. Thus, using shared passwords to protect shared resources such as shared information or shared tasks can be an appropriate means of protection [1]. On the other hand, it has been found that shared passwords sometimes are weak and long lived since the challenges of managing shared passwords discourages good password practices [18], and that users may be more willing to disclose shared passwords [35].

5.2 Barriers and Counter-Measures

As described in Section 3.4 the attack does not exploit technical vulnerabilities. As it turns out, the security of the target INS installation relies heavily on air-gapping and physical protection while the INS itself is quite open once access is established. It is however commonly accepted that this strategy in itself does not provide sufficient security and that the troubles of keeping such systems up do date will contribute to undermine their security [6,22]. In this section we explore various ways to counter the attack, apart from the air-gapping and the physical security.

Security Mechanisms. The operator station under attack was logged in with a user profile with administrator privileges. This was exploited to copy files to the installation folder of the ECDIS software, to make changes to the registry and to create scheduled tasks. The obvious counter-measure is to create a user profile with a more restricted set of privileges for use in the daily operation of the system. This would force the attacker to device a more sophisticated attack with privilege escalation, unless he/she had access to the administrator password (which will have many of the same issues as the ECDIS maintenance password; see Section 5.1). A similar counter-measure would be to disable the Windows Script Host, which is used to execute VBScript.

The operator station did not have anti-virus software installed. According to statements from experts on maritime cyber security this is quite common for INS installations [4]. On the other hand, it is not certain that an anti-virus program would be sufficient to detect and prevent the attack. We submitted our payload to VirusTotal (www.virustotal.com), and only two out of the 60 antivirus programs the service uses to analyze submissions flagged it as unsafe while the remaining 58 flagged it as clean.

More advanced counter-measures would include mechanisms to prevent the fake DLL from loading, and some mechanism to preserve the integrity of the network traffic such as cryptographic signing by the SINT. (See [25] for further discussion on the latter option.)

Redundancy. The INS implements several redundancy features. While these can be considered safety mechanisms, it is still interesting to see if they have any impact on our attack. There are three source of redundancy: A duplication of the LAN, different sensors providing overlapping information, and sensors with serial connections to the operator stations. The dual LAN does not affect the attack since the Winsock DLL reads the network traffic of both LANs. The INS integrates several sensors in addition to the GPS that are also used for positioning such as heading and speed sensors. If the deviation between the GPS position and dead reckoning based on other sensors exceeds a limit, the ECDIS software will sound a Position Deviation Alarm and this may give an indication that there is something wrong with the integrity of the position data. On the other hand, data from the other sensors are transmitted over the network in the same way as the GPS data. It would probably not be very difficult to have the malware manipulate also these data to remove or reduce the deviation from the manipulated GPS data.

The last of the redundancy mechanisms, however, poses a challenge for the attacker. The INS installation on which we tested the attack also has sensors connected to the operator stations using serial connections (seen as the thin blue lines connecting the operator stations to the SINT in Fig. 1). The ECDIS software compares GPS data received over the LAN with GPS data received over the serial connection and sounds the Position Deviation Alarm if the deviation between the two sources of GPS data exceeds a limit. This alarm was in fact sounded during the test runs of our demonstration. To avoid this deviation, the malware would have to manipulate also serial input to the ECDIS software. Since serial input seems to be handled by DLLs, a strategy similar to the manipulation of network traffic should be feasible. However, it would require a more sophisticated malware as manipulation of data across DLLs would need

to be synchronized in some way. An even more sophisticated (but also less feasible) alternative would be a malware installed on the SINT and manipulating the serial input there. On the other hand, the Position Deviation Alarm will only notify the operator that there are discrepancies in the positioning data and will not reveal this as the result of malware.

6 Conclusions

Maritime cyber security is an emerging field, and still the state of cyber security at sea is shrouded behind speculation and anecdotes. There is a need for studies of the concrete systems and threats which populate the maritime domain. Our contribution reported in this paper is the development and demonstration of a cyber attack against an Integrated Navigation System (INS).

We were able to successfully manipulate the GPS position displayed in the ECDIS application of a vessel during a passage. The attack was tailored to the INS and ECDIS delivered by a specific vendor (i.e. the Original Equipment Manufacturer (OEM) of the INS and ECDIS of the vessel). However, a survey of navigation systems shows that many characteristics are shared across vendors and that the INS and ECDIS studied in this paper are fairly typical [25]. We therefore argue that the principles of the attack will apply also to other INS and ECDIS and that similar attacks can be implemented independently of the specific INS and ECDIS products. The attack demonstrated in this paper can in this sense be seen as a representative of a type of attacks against INS and ECDIS.

To the best of our knowledge this kind of attack is novel. Though, cyber attacks manipulating positions displayed in electronic charts have been suggested earlier [11,23], and a demonstration similar to ours was reported in December 2017 [34]. Being a proof-of-concept, the attack has a certain lack of sophistication. However, the investment was less than two person-months of work including the reconnaissance phase; with more resources invested we believe this kind of attack could pose a real threat. On the positive side, we have seen that a combination of technical security measures, physical protection and security policies in many cases can prevent such attacks.

Developing the attack, rather than merely speculating, serves to make explicit its feasibility, consequences and counter-measures. In this paper, these are discussed from a technical perspective. Feasibility, consequences and countermeasures of the attack as seen from the perspectives of navigation and maritime operations are discussed elsewhere [15]. These discussions highlight how maritime cyber security in some respects is similar to cyber security in general and resembles security of SCADA systems, and how it in some respects is a domain that requires domain specific knowledge of both attacker and defender.

Acknowledgement. The work on which this paper reports was partially funded by the Norwegian Armed Forces CD&E grant EP1710 Concepts for CND in joint operations and partially by the Royal Norwegian Naval Academy R&D grant. We want to thank

the provider of the INS and its representatives for supporting the project, and the owner of the vessels and their crews for facilitating our reconnaissance and testing.

References

1. Adams, A., Sasse, M.A.: Users are not the enemy. Commun. ACM **42**(12), 41–46 (1999)
2. Auriemma, L.: Proxocket (2012), http://aluigi.altervista.org/mytoolz.htm#proxocket
3. Balduzzi, M., Pasta, A., Wilhoit, K.: A security evaluation of AIS Automated Identification System. In: 30th Annual Computer Security Applications Conference (ACSAC 2014). pp. 436–445. ACM (2014)
4. Baraniuk, C.: How hackers are targeting the shipping industry. BBC News (Aug 18, 2017), http://www.bbc.com/news/technology-40685821
5. Betke, K.: The NMEA 0183 Protocol (2001)
6. Byres, E.: The air gap: SCADA's enduring security myth. Commun. ACM **58**(8), 29–31 (2013)
7. CyberKeel: Maritime cyber-risks: Virtual pirates at large on the cyber seas (2014)
8. Demchak, C., Patton, K., Tangredi, S.J.: Why are our ships crashing? Competence, overload, and cyber considerations. Center for International Maritime Security (Aug 25, 2017), http://cimsec.org/ships-crashing-competence-overload-cyber-considerations
9. Direnzo, III, J., Drumiller, N.K., Roberts, F.S. (eds.): Issues in Maritime Cyber Security. Westphalia Press (2017)
10. Dyryavyy, Y.: Preparing for Cyber Battleships – Electronic Chart Display and Information Systems Security. NCC Group (2014)
11. Dyryavyy, Y.: Can you hack an ECDIS? United Kingdom Maritime Pilots' Association (Aug 26, 2016), http://ukmpa.org/can-you-hack-an-ecdis-yevgen-dyryavyy/
12. FireEye: Malware Persistence without the Windows Registry (Jul 15, 2010), https://www.fireeye.com/blog/threat-research/2010/07/malware-persistence-windows-registry.html
13. Fitton, O., Price, D., Germond, B., Lacy, M.: The Future of Maritime Cyber Security. Lancaster University (2015)
14. Goward, D.: Mass GPS spoofing attack in Black Sea? The Maritime Executive (Jul 11, 2017), http://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea
15. Hareide, O.S., Jøsok, Ø., Lund, M.S., Helkala, K., Ostnes, R.: Enhancing navigator competence by demonstrating maritime cyber security. Journal of Navigation (2018), to appear
16. Hareide, O.S., Ostnes, R.: Scan pattern for the maritime navigator. International Journal on Marine Navigation and Safety of Sea Transportation (TransNav) **11**(1), 39–47 (2017)
17. Hutchins, E.M., Clopperty, M.J., Amin, R.M.: Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. In: 6th International Conference on Information Warfare and Security (ICIW 2011)
18. Inglesant, P., Sasse, M.A.: The true cost of unusable password policies: Password use in the wild. In: SIGCHI Conference on Human Factors in Computing Systems (CHI 2010). pp. 383–392. ACM (2010)
19. International Maritime Organization (IMO): Resolution MSC.232(82): Adoption of the revised performance standards for Electronic Chart Display and Information Systems (ECDIS) (2006)
20. International Maritime Organization (IMO): Resolution MSC.252(83): Adoption of the Revised Performance Standard for Integrated Navigation Systems (INS) (2007)

21. International Telecommunication Union, Radiocommunication Sector (ITU-R): Recommendation ITU-R M.1371-5 (02/2014): Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band (2014)
22. Johnson, III, R.E.: Survey of SCADA security challenges and potential attack vectors. In: 2010 International Conference for Internet Technology and Secured Transactions (ICITST 2010). IEEE (2010)
23. Jones, K.D., Tam, K., Papadaki, M.: Threats and impacts in maritime cyber security. Engineering & Technology Reference (Apr 22, 2016)
24. Kugler, L.: Why GPS spoofing is a threat to companies, countries. Commun. ACM **60**(9), 18–19 (2017)
25. Lund, M.S., Gulland, J.E., Hareide, O.S., Jøsok, Ø., Weum, K.O.C.: Integrity of Integrated Navigation Systems. In: International Workshop on Cyber-Physical Systems Security (CPS-SEC 2018), to appear
26. Munro, K.: OSINT from ship satcoms (Oct 13, 2017), https://www.pentestpartners.com/security-blog/osint-from-ship-satcoms
27. Norris, A.: Integrated Bridge Systems Vol 1: Radar and AIS. The Nautical Institute(2008)
28. Pavković, N., Perkov, L.: Social Engineering Toolkit – A systematic approach to social engineering. In: 34th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO 2011). pp. 1485–1489. IEEE (2011)
29. PJRC: Teensy USB Development Board, https://www.pjrc.com/teensy
30. Psiaki, M.L., Humphreys, T.E.: GPS lies. IEEE Spectr. **58**(8), 26–32, 52–53 (2016)
31. Raymond, E.S.: AIVDM/AIVDO protocol decoding, version 1.52 (Aug 2016), http://catb.org/gpsd/AIVDM.html
32. Russinovich, M.: PsKill v1.16 (Jun 29, 2016), https://docs.microsoft.com/en-us/sysinternals/downloads/pskill
33. U. S. Coast Guard: Special issue on cybersecurity. Proceedings of the Marine Safety& Security Council, the Coast Guard Journal of Safety & Security at Sea **71**(4) (Winter 2014–2015)
34. Wee, V.: Naval Dome exposes vessel vulnerabilities to cyber attack. Seatrade Maritime News (Dec 22, 2017), http://www.seatrade-maritime.com/news/europe/naval-dome-exposes-vessel-operational-vulnerabilities-to-cyber-attack.html
35. Weirich, D., Sasse, M.A.: Pretty good persuasion: A first step towards effective password security in the real world. In: New Security Paradigms Workshop (NSWP 2001). pp. 137–143. ACM (2001)
36. Wikipedia: NMEA 0183 (Mar 11, 2017), https://en.wikipedia.org/w/index.php?title=NMEA 0183&oldid= 769737723

Necesse 2018, Vol 3, Issue 2, 164-179 DOI: 10.21339/2464-353x.3.2.164

Can you teach an old seadog new tricks? Experimental evaluation of BRM training in the commercial fleet

Sturle Danielsen Tvedt, Western Norway University of Applied Sciences, Simsea Real Operations | sturle.tvedt@gmail.com
Roar Espevik, Royal Norwegian Naval Academy
Helle Asgjerd Oltedal, Western Norway University of Applied Sciences
Guro Persdotter Fjeld, Western Norway University of Applied Sciences
Frode Voll Mjelde, Royal Norwegian Naval Academy

Abstract

Objective: The objective of the present study was to evaluate the effectiveness of Crew Resource Management (CRM) training in the commercial shipping fleet – termed Bridge Resource Management (BRM) training.

Background: CRM training has been widely employed and researched in several high reliability settings. However, there is a lack of experimental studies assessing CRM training in commercial shipping.

Method: An experimental pretest – posttest study measuring satisfaction with training, knowledge, attitudes, and team behavior in bridge simulators. Five hypotheses were made; H1) The BRM training will receive positive evaluation, H2) BRM training will improve knowledge, H3) BRM training will improve attitudes, H4) BRM training will improve behavior, H5) The relationship between Teamwork and Mission success is positively mediated by Situation awareness.

Results: H1 was fully supported. H2 was fully supported. H3 was partly supported. H4 was not supported. H5 was fully supported.

Conclusion: The training was positively evaluated and improved knowledge and some of the targeted attitudes. Behavior could not be shown to improve with statistical significance, but it cannot be ruled out that a stronger experimental design and increased sample size would yield significant results. Relations among behavior measures confirms established CRM theory.

Application: The present study provides supporting evidence that BRM training can indeed improve safety-relevant knowledge and attitudes. However, to improve behavior on the bridge, training should be adapted to specific work procedures.

Introduction

The International maritime organization (IMO) has declared shipping as one of the most dangerous industries in the world (2011). Personnel on board face complex and dangerous machinery, often made worse by heavy sea and challenging navigation. Human errors in this environment can have serious consequences, leading to collisions and explosions with a potential to be both enormous and tragic. The risk becomes even greater when operating far away from first-responder assistance (Hetherington, Flin, Mearns, 2006). To prepare for such a high-risk environment and to avoid accidents, proper training becomes a major concern for maritime organizations (International Maritime Organization, 2002).

Crew Resource Management (CRM) training emerged in the airline industry after several major accidents during the 1970s, when the authorities acknowledged that technical competence alone was not sufficient to guarantee safe performance (Rutherford, Flin & Mitchell, 2012). 30 years later the CRM training has transferred to other high-risk organizations, such as healthcare, military, offshore industry and nuclear plants. In 2010 CRM training became mandatory for the maritime industry in the Manila amendments to the Standards of Training, Certification and Watchkeeping for Seafarers (STCW) regulations (International Maritime Organization, 2011).

However, CRM training is not unproblematic. Despite decades of CRM training of teams in high-risk organizations such as shipping, health care and military there is still considerable uncertainty whether this type of training actually increases safety (Salas et. al., 2006). One reason could be that there seems to be no established agreement as to what CRM training should entail (O'Connor, 2008), making it problematic to transfer training strategies between domains. Musson and Helmreich (2004) underline that CRM training tends to be domain specific, both organizationally and culturally. Specifically, the automatic transplantation of CRM training in aviation to maritime BRM training has been suggested as an explanation for the lack of results within bridge crews (O'Connor, 2011). In the maritime domain, the regulations put forward in 2010 (International Maritime Organization, 2011) makes BRM and ERM training mandatory to achieve maritime certificates. IMO does not however, present or list specific contents for BRM courses in a separate paragraph in the STCW manual. Typical CRM topics are spread out and inserted into various chapters and paragraphs that existed before the 2010 amendments, which make it difficult for instructors and training establishments to construct standardized BRM curriculums.

Despite the domain specific differences, the objective of resource management courses is established through a common conceptual perspective. Salas et. al. (2006) stated in a review that CRM courses (i.e. BRM or ERM in the maritime domain) are intended to increase knowledge, awareness and skills around the importance of clarity of roles, clear communication, and situation awareness. Within this perspective, highly reliable organizations will work towards avoiding accidents by collectively identifying and managing evolving threats. Hence, team members are encouraged to continuously scan for threats and to speak up when they identify potential threats, regardless of their status in the hierarchy or their defined role (Weick, 2002). A CRM course is intended to train and build awareness around teamwork behavior that enhance a common understanding of the situation at hand, eventually resulting in higher performance or mission success. Theoretical perspectives involve individual learning (mental models), teamwork behaviors that enhance and maintain shared mental models and situation awareness (Endsley, 2015, Espevik & Olsen, 2013).

Previous studies have predominantly used undergraduate students (e.g. Stout 1999) or aviator trainees (Salas, E., Cannon-Bowers, Rhodenizer, & Bowers, 1999). Salas, DiazGranados, Weaver, & King (2008) underlined the importance of studying teams in the wild (i.e. when operating their normal job at sea). In the maritime domain, there is a lack of true experimental studies evaluating BRM courses, especially for the commercial fleet. The few existing studies of BRM and related training is either limited to participant satisfaction (Håvold et al., 2015), or to navy samples (O'Connor, 2011; Röttger, 2016).

The present study will examine the effectiveness of BRM training on knowledge, attitudes and behavior in experienced bridge officers through an experimental evaluation of a commercial BRM training program performed for a Norwegian ship owner. The core of this BRM training program evolves around teamwork behavior that builds situation awareness and shared mental models.

Theory

The present theoretical perspective is outlined as an Input-Process-Outcome model (IPO; see Figure 1). The BRM course was constructed and performed to give knowledge about, attitudes towards, and training of, teamwork behavior. This teamwork behavior is understood as Input, which will result in a Process, i.e. better mental models, which enhance Situation awareness (understanding - "what is happening") and Shared mental models (coordination behavior - "what to do"). The outcome of all this is better performance (e.g., mission success).

The input in the BRM course is theoretical and practical training on teamwork behavior. Salas, Sims and Burke (2005) presented a model of teamwork integrating

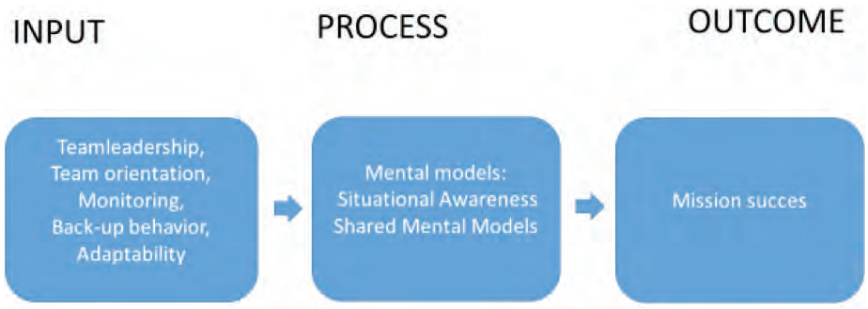


Figure 1. An Input-Process-Outcome model of BRM training.

the most commonly discussed variables that had the greatest effect on team performance. They suggested 5 core components, all of them vital to develop and flourish situational awareness and shared mental models. The first core component is *team leadership*, which entails the ability to direct and coordinate the activities of other team members. Second, *mutual performance monitoring*, which is the ability to apply appropriate task strategies to develop common understanding of the team environment. Third, *backup behavior,* which entails team members' ability to anticipate each other's needs through knowledge about their responsibilities. Fourth, *adaptability,* which concerns the team's ability to adjust team strategies and alter course of action based on information gathered from the environment. The last one, *team orientation* is an attitude characterized by a tendency to take team members behavior and input into account during group interaction, and that team goals are placed above individual goals.

Knowledge about, attitudes towards and training of these teamwork behaviors intends to enhance a team member's mental models of the environment he or she is supposed to operate in. Mental models are the mechanisms whereby humans are able to generate descriptions of a system's purpose and form, explanations of its functioning and observed states, and predictions of future system states (Rouse & Morris, 1986). This is in line with Endsley (2015), as the three stages of Situation awareness (SA) correspond to the three purposes of mental models, namely detecting (elements in the environment), explaining (their meaning) and predicting (their future status).

Endsley (1995) defines situation awareness as 'The perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future'. This indicates that SA is as dynamic as the situation. When new information emerges, SA needs to be updated and changed, thus made possible by the five core teamwork behavior (Salas et.al., 2005). Although Endsley labels SA as a state, it can be argued that she describes three cognitive processes or functions, namely perception, comprehension and projection (Salmon et al., 2006). Perception involves detection of critical signals that are clearly observable and meaningful pieces of information (Level 1). Comprehension (Level 2) involves interpreting and combining relevant perceived information in order to grasp a correct understanding related to a goal. Projections (Level 3) represent forethought where the decision makers predict the status in near future. Thus, SA could be considered as the decision maker's internal model and forms the basis for decisions made. Lack of SA has been stated as the cause of human errors in critical situations. Sneddon, Mearns and Flin (2006) reported that 67% of errors made in their material were caused by lack of Level 1 SA; a failure to detect critical signals. 20 % of the accidents were caused by a lack of correct understanding of the situation (Level 2) and 13% was caused by a failure to correctly predict possible future states of the situation (Level 3). When further investigating the causes of poor SA, the main reason for a failure in Level 1 was found as failure to monitor or distraction causing reduced attention to the task at hand. In addition, a low ability to prioritize the available information resulted in information overload, and critical signals were not detected.

Operational decision making is most often done in a team setting. A related concept to SA is "shared mental models" (SMM). SMM is defined as a shared organized understanding and mental representation of key elements of the team's relevant environment. These shared mental models enable team members to form accurate explanations and expectations of the task. This will in turn enable team members to coordinate their actions and adapt their behavior to the demands of the task and to fellow team members (Converse, Cannon-

Bowers Salas, 1993). SMMs are assumed to enable team members to predict task needs and the actions of other team members, and thus enable them to adapt their own behavior accordingly without communicating explicitly. In a meta-analysis, DeChurch & Mesmer-Magnus (2010) showed a number of studies indicating that SMMs contribute to increased team effectiveness (e.g. Stout, Cannon-Bowers, Salas, & Milanovich, 1999). In a series of simulator studies Espevik, Johnsen, Eid & Thayer (2006) found that operational submarine attack teams with a high degree of SMMs had better performance than other teams. Furthermore, Naval teams with high degree of SMMs showed better coordination and performance when two teams had to coordinate their effort towards a common goal, compared to low SMM-teams (Espevik, Johnsen & Eid, 2011 a). Finally, high SMM teams showed improved learning using cross training in high intensity simulation compared to low SMM-teams (Espevik, Johnsen & Eid, 2011 b). Thus, training focusing on the importance of developing SMMs is important within the maritime domain.

As previously described, CRM training started in the aviation community and quickly spread to other high reliability settings such as armed forces, nuclear energy and healthcare. Since the 1990s healthcare has been the leading domain for research, providing ample evidence for the effectiveness of CRM training (Flin, O'Connor, & Crichton, 2008; Hughes et al., 2016; Weaver et al., 2010). However, when it comes to the maritime domain, studies are scarce. Most of them are set within the surface warfare community (O'Connor, 2011; Röttger et al., 2013; 2016) and the one set in the commercial fleet only deals with the self-reported post training satisfaction (Håvold et al., 2015). Hence, the present study sets out to contribute to the knowledgebase regarding BRM courses for the commercial fleet by evaluating the effectiveness of such a course arranged for a Norwegian ship owner.

Evaluating BRM effectiveness

Kirkpatrick's (1976; 2009) hierarchy is an often-used and valued framework for guiding training evaluation, and consists of four different levels: reactions, learning, behavior and organizational impact (see O'Connor, Campbell, Newon, Melton, Salas and Wilson, 2008; Salas et.al., 2006). This framework entails firstly, *reaction* to cover the degree to which the participants find the time spent worthwhile, or put simply, if they like the training. Secondly there is the level of *learning* which means that the training was understood and absorbed. Learning consists of acquiring knowledge, and personal knowledge is defined as 'the cognitive resources which a person brings to a situation that enable him or her to think and perform' (Eraut, 2000). In assessment terms, learning corresponds to written tests assessing theoretical knowledge. Thirdly, *behavior* is the assessment of whether knowledge learned in training actually transfers to behaviors in a work setting (in our case a work setting in a simulated environment). Fourthly the highest level, *Organizational impact*, to provide evidence for improved safety and effectives in the daily operation of the organization. The findings on the three last levels, learning, behavior and organizational impact are scarce (Salas et.al., 2006), and too our knowledge almost non-existent within the commercial maritime domain.

Hypotheses

There is considerable evidence for self-reports that participants value CRM training (DeChurch, et.al. 2010; Espevik, Saus, & Olsen, 2017) or level one, reaction in the hierarchy proposed by Kirkpatrick (2009). Although it is a very basic indicator of training quality, it is still a necessary part of training, and with the ample evidence in the literature a mean evaluation score higher than "uncertain" is expected.

H1) The BRM training should receive positive evaluation.

Although the few studies most relevant produces mixed evidence for increasing knowledge (O'Connor, 2011; Röttger et al., 2016), the training program evaluated in the present study was informed by these findings. Specifically, O'Connor (2011) presented failing to adapt training to the maritime domain as the cause of his null-finding regarding knowledge. This was a key instructive finding informing the establishment of the present training program, and great care was taken to adapt the training to the maritime domain. In addition, improving knowledge is a key outcome for the present training. Hence, it is reasonable to assume that the BRM training should in fact improve knowledge.

H2) BRM training will improve knowledge.

Both of the most relevant studies showed no evidence for improved attitudes (O'Connor, 2011; Röttger et al., 2016). However, again, O'Connor (2011) failed to adapt training to the maritime domain, and Röttger et al. (2016) only used classroom training. In addition, improving attitudes is a key learning objective for the present training. Hence, we expect the training to improve attitudes.

H3) BRM training will improve attitudes.

No study has yet produced evidence for behavior change by BRM training in the maritime domain. Furthermore, fundamental tenets of the cognitive psychological paradigm would suggest that knowledge and attitudes

are indirect determiners of behavior (Eagly & Chaiken, 1993). However, it has long been an established fact that change in behavior is more difficult than change in knowledge (Hollenbeck, van Knippenberg, & Ilgen, 2017), and this challenge is confounded when applied to a group setting such as in the present study (Lewin, 1943; 1947). Nevertheless, the Kirkpatrick paradigm suggests behavior change as a separate level of evaluation. Furthermore, in the present study, it is of course a main motivation for BRM courses that training teamwork behavior should lead to behavioral change.

H4) BRM-training will improve behavior

According to established theory on the role of Teamwork and situation awareness for Mission success, we expect these behavioral measures to be related at Time 1 (prior to training) and at Time 2 (subsequent to training). In other words: the different behavioral measures are related for each team in each exercise, such that a there is a relationship between a team's Teamwork to their Mission success positively mediated by Situation awareness (see e.g. Espevik et al., 2006; 2011a; 2011b; Stout et al., 1999). See Figure 2. for a conceptual model for H5.

H5) The relationship between Teamwork and Mission success is positively mediated by Situation awareness at each point in time.

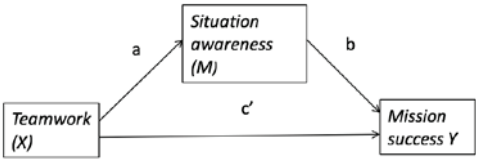


Figure 2. Conceptual model of the relationship of Teamwork mediated through Situation awareness on Mission Success. Conceptual model for the mediation models is showed in the results, tables 5 and 6. Constant coefficients, denoted i_M and i_Y in the table are not represented in the figure as they have only technical statistical interest.

METHODS

Design

The study was set up as a pretest - posttest experimental design. All participants were subject to surveys and simulator tests prior to, and subsequent to, BRM training (see Table 1). All participants received the same theoretical training and practical simulator exercises. Control was achieved with random assignment of the two scenarios (A and B) used for simulation exercises so that one half of participants did A-B and the other half did B-A. Hence, all participants received treatment between pre- and posttest. In addition, random assignment was employed of teams to bridge simulator and assessor for each course week comprising four teams per week. Thus, any variation in execution between course weeks affected each experimental condition equally. Assignment of participants followed a random stratified approach, stratifying according to rank. The result was that most teams had one team member with superior rank to the rest, usually a captain. No teams had junior officers only. Each team consisted of 3 members, except for a minor number of teams with only two participants due to absentees.

Training and Simulator Scenarios

The BRM course consisted of four simulator scenarios in total. The first is a simple transit scenario without critical incidents to familiarize the participants with the simulator. The third scenario was a Search and Rescue (SAR) scenario given the same to all groups as part of the training. The second (scenario A) and fourth (scenario B) scenarios presented were the two scenarios developed specially for the present study, although they could have been used in any regular BRM course: Scenario 2 (A) involved personnel injury on deck in an offshore setting, meaning that the bridge team must make the transition from a standard cargo delivery operation to a critical evacuation of injured personnel, a taxing team effort inducing stress. Scenario 4 (B) involved GPS deviance during a navigational exercise in coastal waters, testing the team's ability to maintain Situation awareness; discovering the GPS deviance through active information gathering and understanding that the GPS derived position is incorrect in the electronic charts (Electronic Chart and Display and Information System – ECDIS).

The total length of the BRM training was five days. According to the Norwegian Maritime Authority's (NMA) interpretation at the time of the international regulations concerning BRM training – Standards of Training, Certification and Watchkeeping for Seafarers (STCW) (International Maritime Organization, 2011), the recommended length of a BRM course was four days. The study included the recommended four days for training, consisting of two days classroom lectures and two days simulation training and observation including feedback sessions – using scenario 3. The pre- and posttests constituted one extra day in duration, bringing this specific course up to five days.

Table 1. Schematic illustration of experimental design.

	Pretest			Training		Posttest	
Randomly assigned Group	Survey 1	Simulator exercise 1[a)]	Simulator exercise 2	Theoretical training	Simulator exercise 3	Simulator exercise 4	Survey 2
1	Knowledge Attitudes	Familari-zation scenario	Scenario A «Stress»	Classroom lecture and discussion	«Search & rescue»	Scenario B «Situation awareness»	Satisfaction Knowledge Attitudes
2	Knowledge Attitudes	Familari-zation scenario	Scenario B «Situation awareness»	Classroom lecture and discussion	«Search & rescue»	Scenario A «Stress»	Satisfaction Knowledge Attitudes

[a)] The familiarization is not a measurement and not the intended experimental manipulation but a necessary preparation of the participants to the equipment on the simulator bridge.

Participants

A total of 94 experienced bridge officers participated in the study, 95.7% men. The age span was 23 to 62, (M=39.9, SD=10.1) and the seniority span was .5 to 34 years (M=6.2, SD=7.2). 35.5% were ranked as captains, 23.7% Chief mates, and 40,9% were first mates. Due to some missing values in either pre- or post-forms, the questionnaire analyses were performed with 79 to 80 participants.

Instruments

Satisfaction: An 8-item rating scale was used as part of the training centre's standard evaluation form. The scale is developed to rate satisfaction with simulation training and contain the following statements: 1) The course was adequate to my previous knowledge. 2) The content held a high professional level. 3) The content was relevant for my work. 4) The simulators are realistic. 5) The simulator exercises are realistic. 6) Our teaching methods are good. 7) Course facilities are satisfactory. 8) All together a good course. A sum score was then computed based on the responses, and the scale had a satisfactory consistency (cronbach's alpha = .78).

Knowledge: A 10-item multiple-choice test was taken with permission from O'Connor (2011) and is described there. A sum score was then computed based on the responses.

Attitudes: A 26 item Ship Management Attiudes Questionnaire (SMAQ) was taken with permission from Andersen, Garay and Itoh (1997). Each statement was followed by a 5-point Likert scale (1 = Fully disagree; 5 = Fully agree). An explorative factor analysis (see Table 2) produced five attitudinal categories: 1) My stress, 2) Stress of others, 3) Communication and coordination, 4) Command and responsibility, and 5) Revealing short comings.

Psychometric analysis

Several variations of SMAQ questionnaires have followed from the original classification of Helmreich and Merrit (1998). However, they do not agree on a common factor structure, which is to be expected from the little extent of actual overlap in items. Hence, the present study needed to establish its own factor structure (see, Andersen et al., 1999; O'Connor, 2011; Röttger et al, 2012). A principal Axis Factor (PAF) with Oblimin (oblique) rotation was run on the SMAQ items at Time 1 and yielded an adequate factor solution explaining 63.6% of the variance. An examination of the s Kaiser-Meyer Olkin measure of sampling adequacy suggested that the sample was favorable (KMO=.675), and Bartlett's test of Sphericity was significant. Eigenvalue's and the scree plot both suggested five factors (see Table 2.)

The are some correlations among the factors both at Time 1 and Time 2, indicating support for an oblique rotation (see Table 3.). In terms of test-retest reliability, the factors correlate around r=.60*** with the exception of factor 3 (Stress of Others), which has a r of =.27*.

In terms of internal consistency, the factors show acceptable values of Cronbach alpha for the first two factors, and increasingly lower factors for the other three, but here the alphas should be considered in light of the low number of items (see Table 3). There is also a decreasing trend from Time 1 to Time 2 in internal consistency, especially with factor 3. This is in some degree expected as the study actively aims to change the attitudes.

Behavior: The behavior was rated by three subject matter experts based on video-recordings of Scenarios A and B. These observers were blind to whether the exercises were performed pre or post training. Three measures of behavior were rated: Teamwork, Situation awareness and Mission success.

Table 2. Factor analysis of SMAQ with factor loadings Time 1.

Factors and items	Factor loadings				
	F1	F2	F3	F4	F5
F1 Communication / coordination					
10. A debriefing and critique of procedures and decisions after critical situations is an important part of safety.	.735				
26. Seniors should delegate responsibilities to junior crews as parts of their training.	.698				
20. Crewmembers should monitor each other for signs of stress or fatigue.	.671				
16. When I detect an error I speak up.	.611				
F2 My stress					
14. I am more likely to make errors in an emergency.		.811			
2. Even when fatigued, I perform effectively during critical times of operation.		-.660			
18. I am less effective when stressed or fatigued		.533			
9. My decision-making ability is as good in emergencies as in routine conditions.		-.449			
F3 Stress of others					
22. Effective team co-ordination requires team members to take into account the personalities of the others participants.			.687		
19. My performance is not adversely affected by working with inexperienced crewmembers			-.539		
4. People should be aware of and sensitive to the personal problems of other crewmembers.			.438		
F4 Command and response					
12. Junior crewmembers should not question their senior officer's decisions.				.558	
1. Senior officers should encourage crewmember questions during normal operations and in emergencies.				-.558	
F5Revaling short comings					
17. I am ashamed when I make a mistake in front of other crewmembers.					.608
3. Asking for assistance makes one appear incompetent.					.511

Extraction Method: Principal Axis Factoring. Rotation Method: Oblimin with Kaiser Normalization. Factors: 1 = Communication /coordination; 2 = My stress; 3 = Stress of others; 4 = Command and responsibility; 5 = Revealing short comings. (Factor loadings =>.40).

Table 3. Correlation matrix of SMAQ factors at Time 1 and Time 2 with internal consistency [(a)].

		Factors Time 1					Factors Time 2.				
		1	2	3	4	5	1	2	3	4	5
Factors Time 1	1	(.71)									
	2	-.081	(.70)								
	3	-.185	-.104	(.50)							
	4	.111	.055	-.079	(.30[b])						
	5	-.254*	.215*	.093	.024	(.29[b])					
Factors Time 2	1	.681***	.119	-.306**	.352**	-.067	(.62)				
	2	.038	.677***	-.157	.124	.240*	.258*	(.55)			
	3	-.331**	-.109	.271*	-.022	-.034	-.406***	-.174	(.15)		
	4	.281*	.249*	-.341**	.591***	-.122	.507***	.322**	-.302**	(.32[b])	
	5	-.154	-.021	.094	-.187	.592***	-.164	.151	.046	-.115	(.23[b])

*[(a)] Cronbach alphas on the diagonal. [(b)] Corrected Item-total correlation. * p < .05, ** p < .01, *** p < .001 (one-tailed)*

Teamwork: to extract teamwork, 8 teamwork constructs of the Royal Norwegian Naval Acadamy (RNoNA) assessment tool was used. The RNoNA assessment tool is designed to assess the performance of military teams participating in complex military training exercises (Mjelde et.al, 2016). The purpose is to evaluate the teams' ability to communicate critical information to maximize collective performance, based on Salas et.al (2006) five teamwork processes. For example, for Backup behavior, Subject matter experts rated the backup behavior they observed by rating the following claim on a 7-point Likert scale from strongly disagree (1) to strongly agree (7): The team showed a high degree of backup behavior, i.e. team members helped/assisted without being asked, or pushed information.

Situation awareness: Two clearly discernable incidents were identified within each scenario. For example, in the "Stress scenario" the first incident was the initial awareness regarding an injury on deck, and the second incident was the subsequent awareness when the situation had evolved to the point when it became clear that helicopter evacuation was 45 minutes away. These incidents were rated by subject matter experts in accordance with Endsley's (1995; 2015) description of levels of situation awareness. For example, perception (quickly perceived the injury), understanding (correctly understood the situation) and prediction (correctly predicted potential outcomes). A mean Situation awareness score was computed from the three observed levels of Situation awareness rated for each incident (six observations in total for each scenario).

Mission success: The same two incidents were also rated as to what degree the teams performed a satisfactory action to control the incident from 1 (strongly disagree) to 7 (strongly agree), in accordance with recommendation of Salas, Tannenbaum, Kraiger, and Smith-Jentsch (2012). A mean score for Mission success was computed from the two incident scores.

Procedure

A questionnaire containing instruments measuring knowledge and attitudes were filled out by the participants prior to- and following the training. The behavior measures were taken during two different scenarios pre- and post-treatment. After being introduced to the course and familiarized with the simulators, the pre-scenario was performed. Following classroom training and a simulator exercise with plenary feedback, the post-scenario was performed.

Participation was based on informed consent and the gathering of data was approved by the Norwegian Data Authority for Social Sciences (NSD).

Table 4. Satisfaction, attitudes, knowledge, and behavior in simulator pre- and post- training with t-tests for change and Cohen's d with 95% Confidence Intervals.

Variable	Time	M	N	SD	t	df	p (one-tailed)	d	95% CI of d
Satisfaction	Post	4.75	80	.548	12.312	79	.000	1.38	[1.08, 1.67]
Knowledge	Pre	5.5250	80	1.79292	-4.368	79	.000	-0.49	[-0.72, -0.26]
	Post	6.5125	80	1.92251					
Communication and coordination	Pre	4.5156	80	.49418	-1.558	79	.062	-0.17	[-0.39, 0.05]
	Post	4.5813	80	.44255					
My stress	Pre	3.3133	79	.78596	-2.388	78	.019	-0.27	[-0.49, -0.04]
	Post	3.4736	79	.67970					
Stress in others	Pre	3.6646	79	.71735	-1.878	78	.032	-0.21	[-0.43, 0.01]
	Post	3.7932	79	.61395					
Command and response	Pre	1.7278	79	.64944	.067	78	.473	0.01	[-0.21, 0.23]
	Post	1.7215	79	.72831					
Revealing short comings	Pre	2.0250	80	.86383	1.027	79	.155	0.11	[-0.11, 0.33]
	Post	1.9375	80	.82052					
Teamwork[a)]	Pre	5.4341	26	1.13751	.045	25	.483	0.09	[-0.30, 0.47]
	Post	5.4220	26	1.24298					
Situation awareness[a)]	Pre	4.5313	24	1.59309	-1.234	23	.118	-0.25	[-0.66, 0.16]
	Post	5.0451	24	1.67714					
Mission success[a)]	Pre	4.6944	24	1.71940	-.288	23	.388	-0.06	[-0.46, 0.34]
	Post	4.8333	24	1.96942					

[a)] *Measures for Teamwork, Situation awareness and Mission Success are given as team values only.*

Hypothesis testing Analyses

The basic analyses, including descriptive, correlations, t-tests, and factor analysis were performed using IBM SPSS version 24.0® for Windows 10®. Effect sizes and 95% confidence intervals for these were computed using the MBESS package, version 3.5.1, with MBESS package version 4.4.3, (Kelley, 2018). H5 was tested with the process macros developed by Hayes (2013) through IBM SPSS 24.bbb0. The macros are based on standard ordinary least squares (OLS) regression (see Figure 2 for a conceptual model). As demonstrated by Preacher and Hayes (2004), this macro produces a test that is more rigorous than that of Baron and Kenny (1986) and at the same time avoids the bias of the Sobel (1982) approach. Preacher and Hayes (2004) achieved this by employing a bootstrapping procedure. Bootstrapping works by basing inferential procedures on concrete sampling distribution from the sample at hand, rather than traditional sampling distribution created by a hypothetical infinite number of samples from the population of interest (Efron, 1982). The concrete sampling distribution thus reflects the distribution of the sample, rendering the assumption of normality superfluous, and allows the testing of mediators on small samples (Preacher & Hayes, 2008). A bootstrap sample of 10,000 was drawn (with replacement) and used for analysis of the mediation model.

Results

Descriptive results are given in Table 4 presenting measures pre- and post-training. The results of the hypothesis testing can be found in tables 4, 5 and 6 and is commented according to the order of the hypotheses given in the introduction.

Table 5. Regression results for the Teamwork mediation model at Time 1 (prior to manipulation) with results for alternative models. Unstandardized OLS Regression Coefficients with Confidence Intervals (Standard Errors in parentheses) Estimating Situation awareness and Mission Success.

	Situation awareness (*M*)			Mission Success (*Y*)		
		Coeff.	95% CI		Coeff.	95% CI
Teamwork (*X*)	$a_1 \rightarrow$	0.736** (0.241)	0.237, 1.235	$c' \rightarrow$	0.342 (0.200)	-0.072, 0.757
Situation awareness (*M*)				$b \rightarrow$	0.812*** (0.146)	0.510, 1.115
Constant	$i_M \rightarrow$	0.925 (1.352)	-1.872, 3.721	$i_Y \rightarrow$	-1.052 (0.954)	-3.032, 0.927
Model Summary	R^2 = .288, F (1, 23) = 9,312**			R^2 = .739, F (2, 22) = 31.082***		
	Bootstrap result for indirect effects					
Indirect effect	*M*		*SE*	LL 95%		UL 95%
Hypothesized Model	0.5981**		0.2262	0.3083		1.1489
Alternative Model 1[d]	0.1339[ns]		0.0933	-0.0232		0.5304
Alternative Model 2[e]	0.0493[ns]		0.1700	-0.5668		0.3846
Alternative Model 3[f]	0.3251[ns]		0.1966	-0.0774		1.0064

**p < .05 **p < .01 ***p < .001. a = the direct effect of X on M. i_M = the direct effect of the constant on M. c' = the direct effect of X on Y. b = the direct effect of M on Y. i_Y = the direct effect of the constant on Y. [d] Situation awareness on Mission Success mediated by Teamwork. [e] Mission success on Teamwork mediated by Situation awareness. [f] Mission Success on Situation awareness mediated by Teamwork.*

H1 posited that the BRM course would be evaluated higher than "uncertain-positive". As illustrated in Table 4, the difference between the mean score and "uncertain-positive" is statistically significant and a large effect.

H2 posited that the BRM course would increase the knowledge. As illustrated in Table 4, the increase in Knowledge is statistically significant and a medium effect.

H3 posited that the BRM course would improve attitudes. As illustrated in Table 4, there is a statistically significant improvement for Stress awareness, Team consideration, and very close to an improvement for Communication and coordination. These are all small effects, and the confidence interval for Communication and coordination includes 0, indicating a likelihood of no effect. The attitudes for Authoritarianism and Weakness toleration, however, showed no statistically significant change. In terms of effect sizes, they are also small to negligible for both of these, the confidence intervals include 0.

H4 posited that the BRM course would improve Behavior. However, there are no statistically significant changes in the behavioral measures. In terms of effect sizes, they are also small to negligible and for all of these, the confidence intervals include 0.

H5 posited that the relationship between Teamwork and Mission success is positively mediated by Situation awareness at each point in time. According to Tables 5 and 6, the hypothesized mediation model was significant at both points in time at alpha level .01 or higher (pre- and post-training). In addition, none of the other possible mediation models were statistically significant.

Table 6. Regression results for the Teamwork mediation model at Time 2 (subsequent to manipulation) with results for alternative models. Unstandardized OLS Regression Coefficients with Confidence Intervals (Standard Errors in parentheses) Estimating Situation awareness and Mission Success.

		Situation awareness (*M*)			Mission Success (*Y*)	
		Coeff.	95% CI		Coeff.	95% CI
Teamwork (*X*)	a →	0.909*** (0.221)	0.454, 1.365	c′→	0.113 (0.181)	-0.262, 0.488
Situation awareness (*M*)				b →	0.886*** (0.128)	0.620, 1.151
Constant	i_M →	-0.364 (1.241)	-2.926, 2.198	i_Y →	0.016 (0.782)	-1.601, 1.633
Model Summary	R2 = .414, F (1, 24) = 16.971***			R2 = .799, F (2, 23) = 45.722***		
	Bootstrap result for indirect effects					
	M		*SE*	LL 95%		UL 95%
Indirect effect	0.8050***		0.2052	0.4949		1.3783
Alternative Model 1[d]	0.0514[ns]		0.0859	-0.0852		0.3446
Alternative Model 2[e]	0.2700[ns]		0.2134	-0.1534		0.5344
Alternative model 3[f]	0.1377[ns]		0.2227	-0.2136		0.5877

**p < .05 **p < .01 ***p < .001. a = the direct effect of X on M. i_M = the direct effect of the constant on M. c′ = the direct effect of X on Y. b = the direct effect of M on Y. i_Y = the direct effect of the constant on Y. [d] Situation awareness on Mission Success mediated by Teamwork. [e] Mission Success on Teamwork mediated by Situation awareness. [f] Mission Success on Situation awareness mediated by Teamwork.*

Discussion

Psychometric analysis

The present study employed a version of the SMAQ but does not entirely replicate the original structure. Instead the present analysis yields a factor structure that closely replicates that of Röttger, Vetter and Kowalski (2013) who's three factors are all represented in the present study (F1, F2, and F4), and even more so O'Connor (2011) who also parcels out F3 from F2. The items of the fifth factor in the present study have elsewhere been placed under F1. However, they are very explicit in their dealing with the revealing of own short comings and invokes the language of shame, hence assigning them to a separate factor makes sense. It could also turn out that this result is due to either the sample being Norwegians, being commercial bridge officers, or both.

Hypotheses

Kirkpatrick's (1976; 2009) recommendations for training evaluation have been widely cited and has also informed the present study. Kirkpatrick (1976; 2009) conceptualizes training evaluation in four levels: 1) Satisfaction, 2) Learning, 3) Behavior change and 4) Organizational outcomes. In the present study, H1 refers to level 1) Satisfaction, H2 and H3 both concerns level 2) Learning, as Kirkpatrick collapses attitudes and knowledge into one level. However, the conceptual separation of attitudes and knowledge is a basic underpinning assumption within cognitive psychology, hence the need for measuring knowledge and attitudes separately should be self-evident. H4 and H5 are concerned with Level 3) Behavior change. Level 4 Organizational outcomes has not been measured in the present study.

H1 posited that the BRM course would be evaluated positively. H1 was fully and substantially supported. This is in accordance with considerable evidence for self-reports that participants value CRM training (DeChurch, et.al. 2010; Espevik, Saus, & Olsen, 2017).

H2 posited that the BRM course would increase the knowledge. H2 was fully and substantially supported. This finding is in accordance with some studies (Röttger et al., 2015), whereas other studies performed in the maritime domain have shown null-results and suggested that this was due to insufficient domain adaptation (O'Connor, 2011). The current support for H2 then, may be seen as supporting O'Connnor's (2011) claim about the importance of domain adapted training.

H3 posited that the BRM course would improve attitudes. H3 was partly supported. As with knowledge, the research literature gives hope, although the most relevant studies for the maritime domain has shown null results (O'Connor, 2011; Röttger, 2015). Again, the adaptation of training to the maritime domain in addition to the fact that the course employed extensive use of simulators in addition to classroom training may in part explain the deviating finding from previous maritime studies (Hobgood et al., 2010; Shapiro et al., 2004). Also, there could be sample particularities at play, since both the other maritime studies employs naval bridge officers. Concerning the varying attitudinal improvement between the five attitude factors, it has been found previously that the different attitudes measured by CMAQ show different proneness to attitude change (Helmreich et al., 1999). Hence, structural differences between the SMAQ versions can also be part of the explanation.

H4 posited that the BRM course would improve Behavior. Sadly, H4 received no support, as the present study failed to produce evidence of behavioral support. This is in accordance with previous studies (O'Connor, 2011; Röttger et al., 2016). However, there are some positive tendencies in the present study that might have proven statistically significant with a larger sample. Here it is prudent to remind the reader that at team level, the present sample is down to N=24/26 for the behavior measures. This is a mere third of the sample size used to test the other hypotheses.

In addition, there are several complicating factors contributing to the present result: 1) For the training to show behavioral change on the team level, the individuals would have to change together in such a way that the group dynamic would change. This could easily be thwarted by other team members either being very good or very poor at the onset. 2) Following requests of the ship owner, the BRM training was carried out in one standard fashion for bridge officers from two vastly different shipping trades. Hence, although random counterbalance of the pre- and post-scenarios were employed, the dramatically different technical skills involved will have diluted any effect of increased non-technical skills on actual behavior. 3) Two out of three raters were professional instructors with commercial maritime practice, without special training in human factors assessment. It is possible that this has contributed to random error, again diluting any effect. 4) Since all assessment were done from video recordings to prevent researcher bias, the assessors were vulnerable to varying quality of both video and audio. This may have centered the assessment scores, which then leads to smaller group differences and smaller effects. 5) Changes in the simulator staff, and occasional technical issues, prohibited full experimental control in the conduction of the scenarios. It should be noted that these are minor issues unproblematic to normal simulator training, but which serves to introduce

potentially substantial random error in experimental measurements. Such random error reduces the internal validity of the experiment and would show up in reduced group differences and smaller, less statistically significant effects.

H5 posited that the relationship between Teamwork and Mission success is positively mediated by Situation awareness at each point in time. H5 was fully supported, adhering to a general input-process-output model where Teamwork is seen as a precursor to Mission success mediated by Situation awareness. (see e.g. Espevik et al., 2006; Espevik et al., 2011a; 2011b; Stout, Cannon-Bowers, Salas, & Milanovich, 1999). That the relationship was fully mediated also underlines the importance of including Situation awareness when assessing outcomes of BRM training, as it gives fuller understanding of the performance of a bridge crew than exclusively focusing on Teamwork and Mission Success.

Limitations

The present sample size is problematic in terms of statistical power for all analysis except the hypothesis testing of H1 regarding training satisfaction and H2 regarding knowledge improvement. Concerning the study's generalizability, the sample is also limited in representing mostly two narrow trades within commercial shipping. However, tugboats and offshore support vessels may be regarded as extremes on a continuum from small to large crews that will envelope much of the crew sizes on most commercial shipping. Also, the inclusion of both offshore maritime operations and coastal navigation in the scenarios makes the sampled exercises generalizable to much commercial shipping. In addition, substantial heterogeneity in the sample in terms of both technical- and non-technical skills have increased random error, which would suggest the sample not to be overly special.

Being part of a commercial course, the experimental control for the present study was less strict than recommended, which constitutes a threat to internal validity, increasing random measurement error and the likelihood of type-two bias in hypothesis testing. However, this lack of experimental control is typical of commercial BRM training, and as such this support claims of external validity.

According to Kirkpatrick's (1976; 2009) recommendations, the study should have included measures of organizational level change. This was dropped early in the design faze as it became clear that it was logistically impossible to follow the performance of the officers as part of their actual bridge teams since they were not coursed together as teams. Furthermore, the evident challenges for revealing any behavioral change in the controlled simulator environment precluded any reasonable expectations of evaluating the same at organizational level (Röttger et al., 2016).

Furthermore, it may be discussed whether long term behavior change belongs to Kirkpatrick's level three or level four. However, as neither the present study nor previous studies have been able to demonstrate even short term behavior change in controlled experimental settings, any long term effects - especially in natural the officers natural environment at work on their own vessels – is unlikely with present training schemes and experimental designs.

Effects of history and training are important to consider for a study like the present where there is no control group not receiving treatment. However, for the theoretical test, the questions are interspersed with four days and no discussion of correct answers were treated, so learning as a bias is unlikely. For the behavioral measure, two different scenarios were used that offered little concrete transference enabling success in the next scenario, other than actually improving resource management skills. Concerning historic effects, five days is a short period of time that is not likely to produce other effects in parallel to the experiment. And lastly, distributing the experiment over eight different weeks over six months with all experimental conditions represented each week should render small chances of random historic changes during the experiment. In fact, no major incidents were reported with shipowner during the six month period of experiment trials.

Regarding H5, a word of caution is necessary in relation to the limitations of OLS regression analyses. It cannot test the causality of the modeled structures, meaning that the directions of relationships given in the models cannot be taken for granted. Alternative causal directions could be possible. For instance, a model was tested that Mission Success had a positive relation to Teamwork, positively mediated by Situation awareness. However, all possible mediations combining these three variables were tested, and none of the alternative mediation models proved significant. A more problematic bias could be introduced by expectations from the observers who were not blind to that particular element of scoring. In other words, they could subconsciously see the different behavior scores of one session in relation. However, in order to fully experimentally control for this, separate observers would have been necessary for the different behaviors.

Regarding the instrument validity, the SMAQ questionnaire proved problematic: The factor loading could still be clearer, with more balance in the number of items for each factor and with higher Cronbach alphas. This may have contributed to random error. Seeing that the two most obviously comparable studies uses two different versions which also have some structural issues, a revision is called for (O'Connor, 2011; Röttger, et al., 2013).

General discussion

Limitations notwithstanding, the present study provides supporting evidence that it is indeed possible to achieve results in resource management training within the maritime domain, in the way it has been shown in other domains (Hughes et al., 2016; Weaver et al., 2010; Espevik, Saus & Olsen, 2017). When the evidence from the literature within the maritime domain has been meager so far, it should perhaps be viewed in connection with certain attributes of the maritime domain: 1) The acceptance of risk in shipping is higher than in other domains such as aviation and medicine (IMO, 2011). 2) The level of academic training amongst practitioners and instructors are comparably low. 3) The adaptation of BRM training within the commercial maritime sector is typically viewed to be relevant for any bridge officer situated within commercial shipping, be it at a one-man fishing vessel, a large super tanker, other tankers- or offshore-related vessels doing highly specialized operations, or different kinds of rigs. The medical equivalent would be to say that the resource management training could use the same scenarios for emergency room surgeons, brain surgeons, and heart surgeons alike. 4) The requirements for resource management training in the maritime domain remain far less strict than in other domains. Currently, the typical course requirements following the 2010 Manilla amendments to the STCW regulations where BRM was for the first time made compulsory, is for a generic three- or four-day BRM course (International Maritime Organization, 2011).

The fact that the present study is capable of showing some improvement in both knowledge and attitude, as well as promising tendencies regarding behavior as well as evidence for the behavioral connection between Teamwork, Situation awareness, and Mission success, supports previous calls for domain-relevant training and the use of simulator training in addition to classroom training (Helmreich et al., 1999; Håvold et al.., 2015; O'Connor, 2011; Röttger et al., 2013; 2016).

It has been noted previously that the level of research on themes relevant for resource management training has been low within the maritime domain, theoretically reducing the value of BRM training (Hetherington, Flin, & Mearns, 2006). Lastly, previous calls to the importance of scientific evaluation of training programs within resource management are as valid as ever, also including the maritime domain (Flin et al., 2008). Furthermore, the principles laid out for such evaluations are readily available and relevant for evidence-based resource management training for commercial bridge officers (Kirkpatrick, 1976; 2009; Espevik et.al. 2017). However, it is presently unclear how organizational change - the last level of evidence in prescribed by Kirkpatrick's classic model – should be measured in practical way as an experimental outcome.

Conclusion

The present study produces evidence that adapted resource management training employing full-mission simulators can indeed be performed to the satisfaction of participants and improve relevant knowledge and attitudes within the maritime domain. Also, there are promising trends, although not statistically significant, that it is possible to improve relevant behavior as measured in a controlled simulator environment. Finally, the present study produces correlational support for the association between Teamwork and Mission success, positively mediated by Situation awareness. Researchers and practitioners alike should aim to specialize the BRM-training for more focused maritime trades and operations. Furthermore, the developments are needed for measuring non-technical skills and safety-relevant behavior at the organizational level in order to connect this outcome to the evaluation of training regimes.

Key Points

- Safety relevant knowledge and attitudes can be improved by Bridge Resource Management (BRM) training.
- Training must be adapted to maritime domain to be effective
- Behavioral change was not significant but could be probably achieved with better customized training design.
- Established resource management training theory concerning mechanisms of team behavior was supported.
- Teamwork was related to Mission Success, mediated by Situation awareness.

Acknowledgments

The authors wish to thank Simsea simulation center and the ship owner for facilitating the present study. The Norwegian Research Council and nine companies in the offshore business in Norway have funded the RISKOP project; Managing Risk in Offshore Operations (grant no.: 225311/O70) at Stord/Haugesund University College, now University of Applied Sciences of Western Norway. UH-Nett Vest, an organization of cooperating Western Norwegian Universities and Colleges, also contributed to the funding of the article. We acknowledge the work of Professor Jan R. Jonassen of the Western Norway University of Applied Sciences (HVL) for finance and facilitation of this research, and Technician Morten Mæland from HVL for facilitation of the exercise recordings.

Statement regarding conflict of interest:

The Main author is employed at the simulation center where the evaluated training has taken place. However, he has not been involved as assessor, and the objective

treatment of data has been monitored by the other authors who have no financial ties with the training provider or the ship owner.

References

Andersen, H.B., Garay, G. and Itoh, K. (1999). Survey data on mariners: Attitudes to safety Issues. Technical Report I-1388, Systems Analysis Department, Risø National Laboratory, DK-4000 Roskilde, Denmark.

Baron, R. B., & Kenny, D. A. (1986). The moderator-mediator distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology, 51,* 1173–1182.

Converse, S., Cannon-Bowers, & J. A., Salas, E. (1993). Shared mental models. In J. N Castellan (Ed.), *Individual and group decision making* (pp. 221-246). Hillsdale, NJ: Erlbaum.

DeChurch, L. A., & Mesmer-Magnus, J. R. (2010). The cognitive underpinnings of effective teamwork: A meta-analysis. *Journal of Applied Psychology, 95*(1), 32.

Eagly, A. H., & Chaiken, S. (1993). *The psychology of attitudes.* Harcourt Brace Jovanovich College Publishers.

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems.*Human Factors, 37* (1), 32-64.

Endsley, M. R. (2015). Situation awareness: operationally necessary and scientifically grounded. *Cognition Technology & Work, 17*, 163-167. doi: 10.1007/s10111-015-0323-5.

Eraut M. (2000). Non-formal learning and tacit knowledge in professional work. *Br J Educ Psychol*.;70:113-136.

Espevik, R., Johnsen, B.H., Eid, J., & Thayer, J. (2006). Shared Mental Models and Operational Effectiveness; Effects on performance and team processes in a submarine attack team. *Military Psychology, 18*, 23-36

Espevik, R.E., Johnsen, B.H., &Eid, J. (2011 a). Communication and Performance in Co-Located and Distributed Teams: An Issue of Shared Mental Models of Team Members? *Military Psychology, 23*, 616–638

Espevik, R.E., Johnsen, B.H., &Eid, J. (2011 b). Outcomes of shared mental models of team members in cross training and high intensity simulations" *Journal of cognitive engeneering and decision making, 5*, 352–377.

Espevik, R., & Olsen, O. K. (2013). A new model for understanding teamwork onboard: The shipmate model. *International maritime health, 64*(2), 89-94.

Espevik, R., Saus, E. R., & Olsen, O. K. (2017). Exploring the core of crew resource management course: speak up or stay silent. *International maritime health, 68*(2), 126-132.

Flin, R. H., O'Connor, P., & Crichton, M. (2008). *Safety at the sharp end: a guide to non-technical skills*. Ashgate Publishing, Ltd.

Hansen, H. L. (1996). Surveillance of deaths on board Danish merchant ships, 1986-93: implications for prevention. *Occupational and environmental medicine, 53*(4), 269-275.

Hayes, A. F. (2013). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach.* New York, NY: The Guilford Press.

Helmreich, R.L. and Merritt, A.C. (1998). Culture at work in aviation and medicine: National, organizational and professional influences. Ashgate, Aldershot, UK.

Helmreich, R. L., Merritt, A. C., & Wilhelm, J. A. (1999). The evolution of crew resource management training in commercial aviation. *The international journal of aviation psychology, 9*(1), 19-32.

Hetherington C, Flin R, Mearns K (2006) Safety in shipping: the human element. J Safety Res 37(4): 401–411. https://doi.org/10.1016/j.jsr.2006.04.007.

Hobgood, C., Sherwood, G., Frush, K., Hollar, D., Maynard, L., Foster, B., ... & Taekman, J. (2010). Teamwork training with nursing and medical students: does the method matter? Results of an interinstitutional, interdisciplinary collaboration. *Quality and Safety in Health Care*, qshc-2007.

Hughes, A. M., Gregory, M. E., Joseph, D. L., Sonesh, S. C., Marlow, S. L., Lacerenza, C. N., ... & Salas, E. (2016). Saving lives: A meta-analysis of team training in healthcare.

Håvold, J. I., Nistad, S., Skiri, A., & Ødegård, A. (2015). The human factor and simulator training for offshore anchor handling operators. *Safety Science, 75*, 136-145.

International Maritime Organization (2011). STCW Convention and STCW Code. International Convention on Standards of Training, Certification and Watchkeeping for seafarers. Including the 2010 Manilla Amendments. London: International Maritime Organization International Maritime Organization.

Wick, K. E., (2002). Safer shipping demands safety culture. Paper presented at the World Maritime Day.

Kelley, K. (2018). *The MBESS R Package.* Date/ Publication 2018-01-10 23:37:02 UTC.

Kirkpatrick DL. (1976). Evaluation. *in* CraigRL (Ed.), *Training and development handbook.* (*pp*. 301–319). *New York: McGraw-Hill*

Kirkpatrick, D. L. (2009). *Implementing the Four Levels: A Practical Guide for Effective Evaluation of*

Training Programs: Easyread Super Large 24pt Edition. ReadHowYouWant. com.
Lewin, K. (1943). Forces behind food habits and methods of change. *Bulletin of the national Research Council, 108*, 35-65.
Lewin, K. (1947). Group decision and social change. *Readings in social psychology, 3*, 197-211.
Mjelde, F. V., Smith, K., Lunde, P., & Espevik, R. (2016). Military teams–A demand for resilience. *Work*, (Preprint), 1-13.
Musson, D. M., & Helmreich, R. L. (2004). Team training and resource management in health care: current issues and future directions. *Harvard Health Policy Review, 5*(1), 25-35.
O'Connor, P. (2011). Assessing the effectiveness of bridge resource management training. *International Journal of Aviation Psychology, 21*, 357–374.
O'Connor, P., Campbell, J., Newon, J., Melton, J., Salas, E., & Wilson, K. A. (2008). Crew resource management training effectiveness: A meta-analysis and some critical needs. *The International Journal of Aviation Psychology, 18*(4), 353-368.
Preacher, K. J., & Hayes, A. F. (2004). SPSS and SAS procedures for estimating indirect effects in simple mediation models. *Behavior Research Methods, Instruments, and Computers, 36*, 717–731.
Preacher, K. J., & Hayes, A. F. (2008). Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. *Behavior Research Methods, 40*, 879–891.
Rouse, W. B. and Morris, N. M. (1986). On looking into the black box: Prospects and limits in search for mental models. *Psychological Bulletin, 100*, 349-363.
Rutherford, J. S., Flin, R., & Mitchell, L. (2012). Non-technical skills of anaesthetic assistants in the perioperative period: a literature review. *British journal of anaesthesia, 109*(1), 27-31.
Röttger, S., Vetter, S. and Kowalski, J.T., (2013). Ship Management Attitudes and Their Relation to Behavior and Performance, Human Factor, 55(3), pp. 659-671.
Röttger, S., Vetter, S., & Kowalski, J. T. (2016). Effects of a classroom-based bridge resource management training on knowledge, attitudes, behaviour and performance of junior naval officers. *WMU Journal of Maritime Affairs, 15*(1), 143-162.
Salas, E., Cannon-Bowers, J., Rhodenizer, L., & Bowers, C. (1999). Training in organizations: Myths, misconceptions, and mistaken assumptions. Research in Personnel and Human Resource Management, 17, 123–161.
Salas, E., DiazGranados, D., Weaver, S. J., & King, H. (2008). Does team training work? Principles for health care. *Academic Emergency Medicine, 15*(11), 1002-1009.
Salas, E., Sims, D. E., & Burke, C. S., (2005). Is there a "big five" in teamwork. *Small Group Research, 36*, 555-599.
Salas, E., Tannenbaum, S. I., Kraiger, K., & Smith-Jentsch, K. A. (2012). The science of training and development in organizations: What matters in practice. Psychological science in the public interest, 13(2), 74-101.
Salmon, P., Stanton, N., Walker, G., & Green, D. (2006). Situation awareness measurement: A review of applicability for C4 i environments. *Applied Ergonomics, 37*, 225-238.
Shapiro, M. J., Morey, J. C., Small, S. D., Langford, V., Kaylor, C. J., Jagminas, L., ... & Jay, G. D. (2004). Simulation based teamwork training for emergency department staff: does it improve clinical team performance when added to an existing didactic teamwork curriculum?. *Quality and Safety in Health Care, 13*(6), 417-421.
Sneddon, A., Mearns, K., & Flin, R. (2006). Situation awareness and safety inoffshore drill crews. *Cognition, Technology and Work, 8,* 255-267.
Sobel, M. E. (1982). Asymptotic confidence intervals for indirect effects in structural equation models. In S. Leinhardt (Ed.), *Sociological methodology* (pp. 290–312). Washington, DC: American Sociological Association.
Stout, R. J., Cannon-Bowers, J. A., Salas, E., & Milanovich, D. M. (1999). Planning, shared mental models, and coordinated performance: An empirical link is established. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 41*(1), 61-71.
Weaver, S. J., Lyons, R., DiazGranados, D., Rosen, M. A., Salas, E., Oglesby, J., ... & King, H. B. (2010). The anatomy of health care team training and the state of practice: a critical review. *Academic Medicine, 85*(11), 1746-1760.
Weick, K. E. (2002). The reduction of medical errors through mindful interdependence. In M. M. Rosenthal & K. M. Sutchcliffe (Eds), Medical error: What do we know? What do we do? (pp.177-199). San Francisco: Jossey-Bass.

Sjøforsvarets Navigasjonskompetansesenter inviterer til

NAVIGASJONSKONFERANSE

NAVIGASJONSKRIGFØRING OG ROBUST NAVIGASJON

Tirsdag 4. desember 2018

Arrangementets foredrag er gradert **HEMMELIG**
Sted: Sjøkrigsskolen, Inge Stenslands auditorium
Registrering fra kl 0800

Avdelingsvis påmelding med sikkerhetsnivå til LT Vibeke Thuesen: vthuesen@mil.no
Sikkerhetsklarering må påtegnes ved påmelding

“Navigare necesse est, vivere non necesse”

Roar Espevik

The quote is attributed to Pompey (56 BC), who used it to urge his sailors on when they refused to set sail on a stormy sea, in order to bring grain from Africa to Rome where people were starving. This is a task familiar to every naval officer: to do his or her duty to society when the situation demands it, is more crucial than own survival. The quote means, literally, “It is necessary to sail, it is not necessary to live”. This means that it is necessary to depart, even if you are not at all sure that you will ever arrive.

It is more “necesse” than ever that we set sail within the academic world. The picture on this last page, the possible monster, Nessie of Loch Ness, symbolizes our quest for knowledge within the naval domain. What is truth? With what kind of certainty can we claim to know the truth? These are central questions whether dealing with a monster or with naval warfare. It is an ongoing process that makes us wiser but not certain. The Royal Norwegian Naval Academy dates back 200 years and the purpose of our magazine is to put our competence, or sometimes even the lack of it, out into the open for debate. We have a threefold wish; to invite to debate and reflection, to present competent arguments, and to publish knowledge gained through peer reviewed research. In short, we have a deep desire to present through “Necesse” our latest academic thoughts, research and efforts concerning anything that is important to a naval officer. “Necesse” will include scientific articles, especially brilliant bachelor papers by our cadets, and works of scholars at our own Academy or others writing within the naval officer sphere.

ISBN 978-82-93550-17-4